

EXHIBIT 50

Mark Graff
2/14/2025

<p>1 UNITED STATES DISTRICT COURT 2 SOUTHERN DISTRICT OF NEW YORK 3 4 SECURITIES AND EXCHANGE) 5 COMMISSION,) 6) 7 Plaintiff,) 8) 9 v.) Case No. 10) 23-cv-09518-PAE 11 SOLARWINDS CORP. and) 12 TIMOTHY G. BROWN,) 13) 14 Defendants.) 15 16 17 18 19 20 21 22 23 24 25</p> <p>VIDEOTAPED DEPOSITION OF MARK GRAFF, taken by the Defendant, pursuant to Notice, held at the law firm of Latham & Watkins LLP, 1271 Avenue of the Americas, 33rd Floor, New York, New York 10020, on February 14, 2025, at 9:45 a.m., before a Notary Public of the State of New York.</p> <p>Reported by: BROOKE E. PERRY JOB No. 250214BP</p>	<p>1 INDEX 2 WITNESS EXAMINATION BY PAGE 3 Mark Graff Serrin Turner 6 4 5 EXHIBITS 6 GRAFF DESCRIPTION PAGE 7 Exhibit 1 Expert Report of Mark G. Graff 20 8 Exhibit 2 Rebuttal Expert Report of Mark G. Graff 20 9 Exhibit 3 SolarWinds Security Statement 63 10 Exhibit 4 Testimony of Mark Graff Vice President, NASDAQ Omx Group Before the House Financial Services Committee Subcommittee on Capital Markets 77 11 Exhibit 5 NASDAQ Omx Provides Updates on Events of August 22, 2013 85 12 Exhibit 6 Statement on NASDAQ Trading Interruption 94 13 Exhibit 7 News Article Entitled NASDAQ: 'Connectivity Issue' Led to Three-Hour Shutdown 96 14 Exhibit 8 NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide 107 15 Exhibit 9 Expert Report of Gregory Rattray 120 16 Exhibit 10 Sw-Sec-Sdny_00048050-095 133 17 Exhibit 11 Sw-Sec-Sdny_00254254-266 160 18 Exhibit 12 7.13.2020 Review 165 19 Exhibit 13 Spreadsheet 166 20 Exhibit 14 Sw-Sec00631418-427 174 21 Exhibit 15 Sw-Sec-Sdny_00050922 188 22 Exhibit 16 Nigel King's LinkedIn Profile 191 23 Exhibit 17 Sw-Sec00012266-275 194 24 Exhibit 18 Transcript Excerpt of Eric Quitugua 197 25</p> <p>3</p>
<p>1 APPEARANCES: 2 ON BEHALF OF THE PLAINTIFF: 3 SECURITIES AND EXCHANGE COMMISSION 4 100 F Street NE 5 Washington, DC 20549 6 BY: CHRISTOPHER J. CARNEY, ESQ. 7 carneyc@sec.gov 8 CHRISTOPHER BRUCKMANN, ESQ. 9 10 ATTORNEYS FOR DEFENDANTS: 11 LATHAM & WATKINS LLP 12 1271 Avenue of the Americas 13 New York, NY 10020 14 BY: SERRIN TURNER, ESQ. 15 serrin.turner@lw.com 16 MATTHEW VALENTI, ESQ. 17 JOSH KATZ, ESQ. 18 19 20 21 22 23 24 25</p> <p>ALSO PRESENT:</p> <p>GREGORY RATTRAY- Expert Witness for SolarWinds</p> <p>JONATHAN JUAREZ-Videographer</p>	<p>1 INDEX (CONTINUED) 2 GRAFF DESCRIPTION PAGE 3 Exhibit 19 Sw-Sec00043620-630 205 4 Exhibit 20 Sw-Sec00386134-143 209 5 Exhibit 21 Sw-Sec00001497-550 215 6 Exhibit 22 Moderate Summary Kp Spreadsheet 231 7 Exhibit 23 Sw-Sec-Sdny_00055077 248 8 9 (Exhibits retained by Reporter.) 10 (EXHIBITS BOUND SEPARATELY.) 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25</p> <p>4</p>

Mark Graff
2/14/2025

<p>1 THE VIDEOGRAPHER: Stand by, please. 2 We are now on the record. 3 My name is Jonathan Juarez. I am a 4 legal videographer for Gradillas Reporting. 5 Today's date is February 14, 2025, and the time 6 is 9:45 a.m. 7 This deposition is taking place at 8 1271 6th Avenue, New York, New York, in the 9 matter of Securities and Exchange Commission 10 versus SolarWinds Corp., et al. The deponent 11 is Mark Graff. 12 Counsel, please identify yourselves for 13 the record. 14 MR. TURNER: Serrin Turner for 15 SolarWinds and Mr. Brown. 16 MS. MELTON: Becky Melton for 17 SolarWinds. 18 MR. VALENTI: Matthew Valenti, Latham & 19 Watkins for SolarWinds. 20 MR. KATZ: Josh Katz, Latham & Watkins 21 for SolarWinds and Mr. Brown. 22 MR. CARNEY: Christopher Carney for the 23 SEC. 24 MR. BRUCKMANN: Christopher Bruckmann for 25 the SEC.</p> <p style="text-align: center;">5</p>	<p>1 Q. Let me ask you first about your current 2 business. You have a business called Tellagraff, LLC; 3 is that right? 4 A. Yes, that's right. 5 Q. And can you just tell me what services you 6 provide to clients in that business? 7 A. Well, I'm doing expert business work. I've 8 done some consulting, cybersecurity consulting for small 9 businesses, and under that rubric also, I'm a 10 professor -- an adjunct professor at the University of 11 Arkansas Little Rock. 12 Q. When you say you've done some consulting for 13 small businesses, what sort of small businesses are we 14 talking about? 15 A. Oh, there was a shop that had -- made metal 16 disks, right. A little shop of a few people. There are 17 folks that operate cafes, you know, catering businesses, 18 that sort of thing. 19 Q. Are these local businesses in Arkansas? 20 A. Well, I just moved to Arkansas recently. Most 21 of that was actually -- some of that was in 22 Philadelphia, Pennsylvania, some of it was in New York, 23 and a little bit of Arkansas. 24 Q. But they were local businesses in those 25 locations?</p> <p style="text-align: center;">7</p>
<p>1 THE VIDEOGRAPHER: The court reporter 2 is Brooke Perry and will now swear in the 3 witness. 4 M A R K G R A F F, the witness herein, having been 5 first duly sworn by a Notary Public of the State of New 6 York, was examined and testified as follows: 7 THE REPORTER: Please state your name 8 for the record. 9 THE WITNESS: Mark Gregory Graff. 10 THE REPORTER: Please state your 11 address for the record. 12 THE WITNESS: 415 North Washington 13 Avenue, Fayetteville, Arkansas 72701. 14 EXAMINATION BY 15 MR. TURNER: 16 Q. Good morning, Mr. Graff. 17 A. Hi. 18 Q. So you understand you're testifying under oath 19 today, right? 20 A. Yes, mm-hmm. 21 Q. So you have an obligation to be truthful just 22 as much as you would if you were testifying in court. 23 You have to answer yes or no. It's for the court 24 record. 25 A. I understand.</p> <p style="text-align: center;">6</p>	<p>1 A. Well, when I was living in New York, I did some 2 work for some folks in -- near Philadelphia, but 3 generally speaking, it's been local, people I know 4 usually. 5 Q. How many clients has Tellagraff, LLC had over 6 the period of time it's been in operation? 7 A. Oh, probably half a dozen all together, maybe 8 even fewer. 9 Q. It's been in business since 2015? 10 A. That's right. I started just as I left NASDAQ. 11 Q. So about six clients every eight years? 12 A. Something like that. 13 Q. And what have you done for them exactly? 14 A. Well, I mean, I've also written another book. 15 As I said, I've done -- I'm working as an adjunct 16 professor at University -- 17 Q. I'll just interrupt you because I'm just asking 18 what did you do for these half dozen clients. 19 A. Okay. And I'll just finish my sentence. 20 I was doing some consulting work but also doing 21 the professorial work, so I count that as part of the 22 company. 23 Mostly it's a matter of -- I had -- they also 24 did a radio show for a few years. So the idea is 25 talking to people who run small business, finding out,</p> <p style="text-align: center;">8</p>

<p>1 you know, I ask them how many computers they have, what 2 they use, and I give them some general advice about how 3 to protect themselves and their systems, their data. 4 Q. And these companies, you said they're small 5 businesses, so what does that mean, like 10 employees, 6 20 employees, that general range? 7 A. Sure. Even smaller sometimes. 8 Q. Have you ever done any cybersecurity 9 assessments under any industry frameworks for these 10 businesses? 11 MR. CARNEY: Objection. Vague. 12 Q. You still have to answer. 13 A. Sure. Thank you. 14 One or two of the clients I did cybersecurity 15 assessments, mostly informal. 16 Q. Mostly informal. Can you explain what you mean 17 by that? 18 A. Sure. There are different levels of 19 formalities you can use when you do cybersecurity 20 assessments. You could use the NIST frameworks and the 21 NIST instruments. You could use -- some of the 22 recommendations from the Federal Trade Commission are 23 very useful in terms of guidance for small business. 24 There's the CISA, Cybersecurity Infrastructure Security 25 Agency. They have a set of recommendations.</p> <p style="text-align: center;">9</p>	<p>1 some thoughts about cybersecurity. 2 Q. You did informal cybersecurity assessments over 3 the air? 4 A. I did, yeah. 5 Q. Did have people calling in asking for 6 cybersecurity assessments? 7 A. Yes, that's one of the ways we did it. 8 Q. What's some examples of the sorts of questions 9 they'd ask? 10 A. Oh, gosh. Well, some of the questions were 11 what kind of antivirus software should I be running? Do 12 I have to worry about ransomware? We talked a lot of 13 about ransomware and that sort of thing. So they were 14 mostly interested in what could go wrong, where the 15 attacks might come from, what kind of losses we might 16 incur. We talked sometimes about cybersecurity 17 insurance and so forth. I never endorsed particular 18 products, but I would give them general guidance about 19 what they could do. 20 Q. Okay. But is it fair to say those weren't 21 really cybersecurity assessments; those were just 22 answering one-off calls from listeners about their 23 questions they have -- 24 A. Well -- 25 Q. If you could just let me finish my question</p> <p style="text-align: center;">11</p>
<p>1 So it depends. You have to fit the instrument 2 you're going to use and the methodology you're going to 3 use with the personalities and the nature of the 4 business. A lot of these small businesses people don't 5 really want to see a big formal analysis with big 6 spreadsheets. They want to talk to you about what 7 they're doing and what their problems might be. 8 Q. So did you use any of the frameworks you just 9 mentioned in conducting your assessments? Or was it -- 10 let me just finish my question. 11 Or was it more informal in the sense, like, are 12 you, you know, running antivirus, it would be a good 13 idea to run antivirus, sort of that level of 14 informality? 15 MR. CARNEY: Objection to form. 16 A. Generally speaking, these small business 17 assessments have been informal. Along the lines you 18 have mentioned, I talk to them about their computers, 19 what they use the business for, what did they do, how 20 many employees do they have, who has accounts on them, 21 how do they manage their accounts. Preponderance of the 22 small business. 23 And, of course, I did -- as I said, I did the 24 radio show, so I did informal assessments over the air, 25 just, you know, just 5 or 10, 15 minutes giving them</p> <p style="text-align: center;">10</p>	<p>1 before you answer. But go ahead. 2 MR. CARNEY: Objection to form. 3 THE REPORTER: I think you want to 4 repeat the question. 5 MR. TURNER: Sure. 6 Q. So fair to say that when you are talking on the 7 radio, you're not doing what would be considered in the 8 industry as cybersecurity assessments, but you're really 9 just responding to listener questions about 10 cybersecurity? 11 MR. CARNEY: Objection. Compound. 12 A. Sure. It's an informal assessment, a 13 conversation really at that level. 14 Q. Okay. And so fair to say, in terms of the 15 business you've done at Tellagraff, that you have not 16 done cybersecurity assessments under recognized industry 17 framework like NIST or CISA, but instead you've done 18 more informal assessments as you described earlier? 19 MR. CARNEY: Objection to form. 20 A. Yes. Since leaving NASDAQ, I think that's the 21 case that they've all been relatively informal 22 assessments. I don't recall doing a big formal 23 assessment using those instruments since I left NASDAQ. 24 Q. And you said you teach currently? 25 A. Yes.</p> <p style="text-align: center;">12</p>

<p>1 Q. Let's take a look at paragraph 47, if we can.</p> <p>2 A. Sure.</p> <p>3 Q. You say, in 47:</p> <p>4 "It is also important to observe that</p> <p>5 many of the assertions in the Security</p> <p>6 Statement were categorical and unqualified."</p> <p>7 A. Mm -- hmm.</p> <p>8 Q. (READING):</p> <p>9 "The Security Statement contained</p> <p>10 little qualifying language indicating the</p> <p>11 assertions of the Security Statement might not</p> <p>12 be consistently followed. For example, while</p> <p>13 the Security Statement noted that 'SolarWinds</p> <p>14 strives to apply the' least -- "'the latest</p> <p>15 security patches and updates,' it did not use</p> <p>16 similar language (such as 'strives') with</p> <p>17 respect to the other assertions. In fact, many</p> <p>18 sentences explicitly used language indicating</p> <p>19 categorical assertions, such as 'By default,</p> <p>20 all accesses is denied,' 'Our password policy</p> <p>21 covers all applicable information systems,' and</p> <p>22 'Quality Assurance is involved at each phase of</p> <p>23 the lifecycle, and security best practices are</p> <p>24 a mandated aspect of all development</p> <p>25 activities.'"</p> <p style="text-align: center;">25</p>	<p>1 I'm not talking about the practices as being</p> <p>2 categorical or unqualified; that wouldn't make any</p> <p>3 sense. So I'm talking about the assertions in the</p> <p>4 security statement, did they have qualifications or as I</p> <p>5 show, does it say something like all access is denied.</p> <p>6 That's what I mean by categorical and unqualified.</p> <p>7 Q. I'm asking you, sir, what you understand the</p> <p>8 implication of the categorical language to mean. Do you</p> <p>9 mean it to imply that SolarWinds is representing that it</p> <p>10 always does these things?</p> <p>11 A. No. When they make a categorical statement, it</p> <p>12 doesn't necessarily imply that they do it 100 percent of</p> <p>13 the time, as I say in the report, I'm sure in the</p> <p>14 paragraph right nearby.</p> <p>15 Q. So then why does it matter whether the language</p> <p>16 is categorical or not?</p> <p>17 A. If they say that they -- by default all access</p> <p>18 is denied, they're making an assertion that all access</p> <p>19 is denied.</p> <p>20 Q. Without exception?</p> <p>21 A. They're making an assertion that all access is</p> <p>22 denied. Now, of course, and I have -- I carefully</p> <p>23 described this is in my report and we can find it, I'm</p> <p>24 not talking about perfect security, I'm not talking</p> <p>25 about something being done 100 percent of the time.</p> <p style="text-align: center;">27</p>
<p>1 And then you say:</p> <p>2 "Based on my experience with security</p> <p>3 statements and how organizations discuss</p> <p>4 cybersecurity practices, when organizations</p> <p>5 make such categorical and unqualified</p> <p>6 assertions about their cybersecurity practices,</p> <p>7 I interpret this to mean that such practice are</p> <p>8 consistently followed."</p> <p>9 Here's what I want to focus on: That last</p> <p>10 statement, are you saying that when you see categorical</p> <p>11 language, you interpret it to mean that the practices</p> <p>12 are categorically followed, meaning without exception?</p> <p>13 MR. CARNEY: Objection. Misstates the</p> <p>14 report.</p> <p>15 MR. TURNER: You may answer.</p> <p>16 A. Well that's not -- that's not the way I use the</p> <p>17 word "categorical," but I also want to point out that</p> <p>18 when you read that paragraph, you did leave out one</p> <p>19 word. I think -- because I said covers all -- what I am</p> <p>20 saying password policy covers all applicable information</p> <p>21 systems.</p> <p>22 But going back to your question about</p> <p>23 categorical, I use that word when I'm talking about if</p> <p>24 there are assertions in the security statement that are</p> <p>25 not qualified as to the extent those assertions apply.</p> <p style="text-align: center;">26</p>	<p>1 What I'm looking for is are the assertions in the</p> <p>2 security statement consistent with the practices that</p> <p>3 they actually on the ground did, as expressed in the</p> <p>4 e-mails and the reports and the presentations and the</p> <p>5 other internal evidence.</p> <p>6 Q. Sir, you put a lot of emphasis on what you call</p> <p>7 "categorical language." I'm just trying to understand</p> <p>8 why do you think that is significant. You say you don't</p> <p>9 construe categorical language to mean that SolarWinds</p> <p>10 does something 100 percent of the time; is that right?</p> <p>11 MR. CARNEY: Objection to form.</p> <p>12 A. I think what I'd like to do is --</p> <p>13 Q. Can you just answer my question, sir.</p> <p>14 A. I certainly will. And let me see if I can find</p> <p>15 quickly the exact way I expressed this. Because I was</p> <p>16 very careful in that language. So in paragraph 48, for</p> <p>17 example, I said:</p> <p>18 "I am of the opinion that the state of</p> <p>19 cybersecurity depicted in SolarWinds' internal</p> <p>20 discussions did not match several of the very</p> <p>21 broad, categorical and unqualified assertions."</p> <p>22 So what I said in that paragraph is several of</p> <p>23 the cybersecurity issues raised in the internal</p> <p>24 documents and these internal documents indicate that</p> <p>25 SolarWinds failed to consistently apply the</p> <p style="text-align: center;">28</p>

Mark Graff
2/14/2025

<p>1 cybersecurity practices described in the security 2 statements.</p> <p>3 So you see what I'm saying is that when they 4 make unqualified statements, assertions in the security 5 statement, and then I compare that to what they actually 6 did on the ground, what actually happened, I find that 7 they didn't consistently apply those practices.</p> <p>8 Q. I'm just trying to understand what you mean by 9 the words you're using. So consistently, what does 10 consistently mean? Does that mean 100 percent of the 11 time?</p> <p>12 MR. CARNEY: Objection to form.</p> <p>13 A. If they do it consistently means they do it 14 with consistency. They do it as a -- as a regular 15 practice. They do it, not 100 percent of the time, but, 16 you know, there are so many examples that I give in this 17 report of major oversights, major areas, significant 18 areas where they deviated from what they said they were 19 doing. It's those significant deviations that I find 20 were not consistent with their assertions.</p> <p>21 Q. A couple of things that I want to unpack there. 22 So you say by "consistently" you mean do something as a 23 regular practice, fair?</p> <p>24 A. I don't know that I would define it quite that 25 way, but that --</p> <p>29</p>	<p>1 definition. That's certainly one of the ways in which 2 you can be consistent and to do something as a regular 3 practice.</p> <p>4 Q. I'm asking you what you meant by it. I'm 5 trying to understand what your conclusions are, 6 Mr. Graff, because you repeat this phrase repeatedly in 7 your report, that SolarWinds didn't do things 8 consistently. And I want to understand what it means. 9 Is your opinion, for example, that SolarWinds 10 did not have a regular practice of having role-based 11 access controls?</p> <p>12 MR. CARNEY: Objection to form.</p> <p>13 A. I found in the evidence many indications that 14 they had not performed access control as they said they 15 did and as they said they were doing it.</p> <p>16 Q. And we'll talk about the evidence that you rely 17 on, but I want to understand your conclusion, because 18 when you say SolarWinds didn't do this consistently, are 19 you saying that they did not do it as a regular 20 practice? Is that what "consistently" means?</p> <p>21 A. Gee, I don't know that I can define it as quite 22 being equivalent to -- to that phrase. It's certainly 23 something -- if you do consistently and you do as a 24 matter of regular practice, that's one of the ways you 25 can do it consistently, but there are many other ways</p> <p>31</p>
<p>1 Q. Mr. -- I'm just repeating the exact words. I 2 can read them back, if you'd like. But you said -- I 3 asked you, "Does it mean 100 percent of the time?" You 4 said, "No, I don't mean that. I mean as a regular 5 practice." I just want to get a clear answer for the 6 record.</p> <p>7 When you say "consistently," are you referring 8 to doing something as a regular practice?</p> <p>9 A. I wouldn't say that's a precise definition of 10 the word "consistently."</p> <p>11 Q. Well, then what does it mean, Mr. Graff?</p> <p>12 A. Okay. You're asking me what the word 13 "consistently" means as I use it.</p> <p>14 Q. Yes.</p> <p>15 A. When I look at the evidence, I see that there 16 were significant deviations, significant variations from 17 what they said they were going to do, what they said 18 they did, and so when there are significant deviations 19 in the evidence, to me, that means that what they were 20 doing wasn't consistent with their assertion in the 21 security statement.</p> <p>22 Q. Meaning you concluded from these supposed 23 deviations that SolarWinds did not do these things as a 24 regular practice?</p> <p>25 A. I'm not quite sure I would say that as an exact</p> <p>30</p>	<p>1 you can do it consistently too.</p> <p>2 Q. So can you not define for me what you mean and 3 the terms that you use for your conclusions?</p> <p>4 MR. CARNEY: Objection. Argumentative, 5 asked and answered.</p> <p>6 A. The best answer I can give you is that when I 7 looked at the evidence, that I find that when there -- 8 as as many significant exceptions and variations and 9 mistakes as I see, then I conclude that they weren't 10 doing it consistently.</p> <p>11 Q. So it's based on there being many instances of 12 noncompliance; is that what you're finding when you say 13 they didn't do something consistently?</p> <p>14 MR. CARNEY: Objection to form.</p> <p>15 A. When I look at the many instances of problems 16 and the reports internally of things that went wrong 17 with regard to access control, user authentication, and 18 so forth, I conclude that they weren't consistently 19 performing in a manner that aligns with the categorical 20 and unqualified assertions in the security statement.</p> <p>21 Q. And I just want to be clear, basically you're 22 saying you found many examples of noncompliance, and 23 based on that, your conclusion is that these practices 24 weren't consistently followed?</p> <p>25 MR. CARNEY: Objection. Vague.</p> <p>32</p>

<p>1 Q. I just want to understand, is the "many" a part 2 of it? Does your finding depend -- does your conclusion 3 depend on your finding that there were many examples of 4 noncompliance?</p> <p>5 A. I wouldn't say my conclusion depends on my 6 finding. There were -- there were so many examples in 7 the evidence I examined where SolarWinds employees, some 8 of them directly responsible for the cybersecurity at 9 the company, said that they weren't doing access control 10 correctly or they weren't consistent with passwords and 11 they had problems in putting passwords in configuration 12 files. They had -- they had inappropriate access 13 between their system and customer systems.</p> <p>14 So these employees were pointing out these 15 problems, and because of that evidence and other, I 16 concluded that with regard to those areas I'm talking 17 about, the performance at SolarWinds was not consistent 18 with the statements that were unqualified, that talk 19 about something being mandated, something happening all 20 the time.</p> <p>21 So with regard to those unqualified assertions 22 in the security statement, I found that the reports 23 where the employees showed the problems, the employees 24 talked about their lack of consistency in access control 25 and so forth, that leads me to conclude that these</p> <p style="text-align: center;">33</p>	<p>1 So if the state of cybersecurity was consistent 2 with SolarWinds' internal assessments, why would it 3 matter whether they were also consistent with industry 4 norms?</p> <p>5 MR. CARNEY: Objection to form.</p> <p>6 A. I'll answer that question. Let me begin by 7 reading the paragraph 17 --</p> <p>8 Q. We've already read it, Mr. Graff, so if you 9 could just answer my question.</p> <p>10 A. We have, but you paraphrased it, so I am going 11 to give you the precise wording here. It says that what 12 I was supposed to do, to continue:</p> <p>13 "Is a technical comparison between the 14 state of cybersecurity depicted in the security 15 statement and communications" and so forth, 16 "regarding the state of cybersecurity during 17 that same timeframe with respect to these five 18 areas."</p> <p>19 I won't read all five areas -- but you notice 20 that the fifth area that I was given in the original 21 assignment was adherence to the NIST cybersecurity 22 framework.</p> <p>23 Well, as I discuss in my report, I wasn't able 24 to tackle that head-on because of the nature of the NIST 25 cybersecurity framework. And I think, yes, in paragraph</p> <p style="text-align: center;">35</p>
<p>1 categorical statements that I call out in the report 2 were not consistent with what was actually happening on 3 the ground.</p> <p>4 Q. Okay. Let's talk about the evidence that you 5 looked at and the next step in your analysis.</p> <p>6 A. Mm-hmm.</p> <p>7 Q. In terms of -- let me actually back up, because 8 the second step in your analysis, and we can go back to 9 paragraph 45, is that you say you evaluated whether:</p> <p>10 "The practices described in the 11 verifiable/falsifiable assertions were 12 consistent with widely accepted norms."</p> <p>13 Now, why did that matter to your analysis? As 14 I understand it, you were trying to find out whether 15 SolarWinds did these things, not whether they conformed 16 to widely accepted norms. So I'm curious why you 17 factored this into your analysis.</p> <p>18 MR. CARNEY: Objection to form.</p> <p>19 A. To answer that question I have to go back to my 20 assignment because, as part of that, I can explain why I 21 took that approach.</p> <p>22 Q. So your assignment is to determine -- as you 23 put it, to compare the state of security depicted in the 24 security statement to SolarWinds' internal assessments, 25 presentations, and communications.</p> <p style="text-align: center;">34</p>	<p>1 21 and so forth, I talk about the NIST cybersecurity 2 framework. Because the NIST cybersecurity framework is 3 not precisely a standard, it wasn't -- I wasn't able to 4 evaluate directly the assertion in the security 5 statement that they followed, and that was the word in 6 the security statement, the cybersecurity framework.</p> <p>7 So what I decided to do was -- and I talk in paragraph 8 21 and so forth about the cybersecurity framework in 9 some length. But what I say in 22 is -- and here we go 10 -- here's the response to your question:</p> <p>11 "Because I consider the assertion that, 12 'SolarWinds follows the NIST Cybersecurity 13 Framework' not to be verifiable or falsifiable, 14 I did not undertake a separate analysis 15 regarding SolarWinds' adherence to the NIST 16 Cybersecurity Framework. Instead, I considered 17 whether SolarWinds followed cybersecurity norms 18 and best practices in my analysis of the other 19 four areas."</p> <p>20 So to answer your question, the reason that I 21 considered these norms were relevant to this -- to this 22 report is because I couldn't directly evaluate that 23 phrase that says they followed the cybersecurity 24 framework. But since the cybersecurity framework is one 25 of the strongest expressions of norms in cybersecurity,</p> <p style="text-align: center;">36</p>

<p>1 then I was able to say, well, let me compare it to -- 2 compare these statements and their performance to 3 industry norms and best practices. Of course, in the 4 security statement they do refer to best practices, 5 industry practices, industry standards and so forth. So 6 I felt that that was the best way to tackle this part of 7 my assignment. 8 Q. Okay. We're going to come back to the NIST 9 cybersecurity framework later, so let's bracket that. 10 Let's move on to the third step in your 11 analysis, which is your actual evaluation. You say in 12 paragraph 45(C) that you: 13 "Created a set of keywords and terms 14 that, based on my experience, I considered to 15 relate to each of the four areas I have been 16 assigned to investigate. I asked my team to 17 search the production documents for these 18 terms." 19 What were the keywords you selected to search 20 through the production documents? 21 A. I can give you some examples. I don't have a 22 precise list of them because it was an iterative 23 process. I'll be glad to describe the process in more 24 detail. But we looked for -- for example, if I'm trying 25 to understand SolarWinds' practices with regard to</p> <p style="text-align: center;">37</p>	<p>1 reviews of the documents after you're searching for 2 them? 3 MR. CARNEY: Objection. Vague. 4 A. They had access to -- there was a repository of 5 SEC documents. They are the ones that actually did the 6 searches, producing documents. They did not review the 7 documents. I was reviewing the documents. But they 8 performed the literal searches in most cases. 9 Q. So they would just run the search terms and 10 then give you documents in bulk to review yourself? 11 A. Well, I had lots of documents to review, of 12 course, and some of them were given to me directly, so 13 there were documents that didn't require any searches. 14 But there are others that were the results of the 15 keyword searches that Analysis Group did at my 16 direction, and they relayed those documents to me. 17 Q. Basically, what I'm trying to get at, sir, if 18 you said search for access controls, for example, did 19 they pull up all documents related to access -- 20 referencing access controls and then you would yourself 21 review those and pick the ones that were relevant, or 22 were they filtered for you somehow before you reviewed 23 them? 24 A. Well, I gave them direction as to, not only the 25 terms, but, I mean, if somebody had a document that</p> <p style="text-align: center;">39</p>
<p>1 access controls, we looked for the words "access 2 controls" in these documents. We looked for the words 3 "user identification," we looked for the words 4 "passwords." 5 So I gave them a set of keywords that were 6 directly related to the assignment as a start, and then, 7 as we began to get more and more information from the 8 documents that we -- were located but also the documents 9 that were supplied to me in regard to the -- I'm sure 10 we'll talk about the so-called SARFs, the forms, the 11 S-A-R-Fs, and the risk acceptance forms and the other 12 documents. As I began to examined those, I found other 13 areas I wanted to explore, and so I gave them additional 14 keywords. We did searches on the SARF, we did searches 15 on -- we talked about -- we referred to Tim Brown or 16 Mr. Colquitt, Mr. Quitugua, and so forth, when we began 17 looking at documents, what they had discussed things. 18 We looked at those names, we looked at -- for policies 19 and so forth. 20 Q. Okay. And your team, who is your team that you 21 are referring to here? 22 A. There was a team that was assisting me. They 23 are from a company called the Analysis Group, which is 24 an economic and litigation support company. 25 Q. And are they the ones that are doing the</p> <p style="text-align: center;">38</p>	<p>1 said, Gee, we really ought to talk about access 2 controls, and they happen to have those two words, or 3 they talked about passwords, a lot of people talked 4 about passwords. Maybe there was a document that 5 referred to passwords, but just in passing, I didn't, as 6 a rule, want to see those. They showed me a whole lot 7 of them, but I did direct them that if there were 8 incidental references in a file, that I didn't 9 necessarily see every file. I may have seen every file 10 that had the word "password" in it, I think there were 11 an awful lot of them. 12 Q. Did you give them any guidance in terms of 13 looking for, let's say, issues of noncompliance or were 14 you looking for anything relating to passwords so that 15 you also saw examples of compliance? 16 MR. CARNEY: Objection. Compound. 17 A. I didn't give them any direction with regard to 18 that kind of substantive issue of noncompliance or 19 compliance. 20 Q. So anything related to access controls, for 21 example, documentation showing there's access controls 22 being followed on a day-to-day basis, you would have 23 gotten information about that just as much as you would 24 have an example of access controls being flagged as a 25 problem?</p> <p style="text-align: center;">40</p>

Mark Graff
2/14/2025

<p>1 MR. CARNEY: Objection. Form. 2 Q. You can tell me if I need to restate my 3 question. 4 A. Well, I certainly didn't give any direction 5 regarding how they should filter -- only look for 6 negative stuff. Absolutely not. I mean, what I was 7 trying to do was form an accurate picture of what the 8 SolarWinds' documents reflected about these areas I was 9 investigating. 10 Q. And I think you said in your assignment you 11 were given, going back to paragraph 17, that you were 12 supposed to look at internal assessments, presentations, 13 and communications regarding the state of cybersecurity? 14 A. Yeah, that's right. That's what it says. 15 Q. So are those the only documents you looked at, 16 internal communications, presentations, and 17 communications? 18 A. No. There were plenty others. As I said, I 19 didn't know at the time that I started that I would be 20 looking at dozens of -- I think they are SARFs -- I 21 think that's System Access Request Form -- I didn't know 22 I was going to be looking at all those. I looked at 23 quite a few of those. I looked at risk acceptance 24 forms. So there were things other than e-mails. There 25 were also a lot of forms and then reports and so forth.</p> <p>41</p>	<p>1 with regard to the cybersecurity in this area. 2 Q. And you would want any relevant evidence 3 regardless of whether it was a communication, 4 assessment, or presentation, right? 5 A. I didn't limit myself to those three things. 6 Q. Okay. So you mentioned in paragraph 45(C) that 7 "Counsel provided me with risk acceptance forms." 8 So that's one type of document you asked for? 9 A. Well, after I knew that they existed, I asked 10 to see many of them, yes. 11 Q. And you knew they existed from testimony, 12 right? 13 A. That sounds right, yes. 14 Q. You reviewed all the testimony in the case, I 15 assume? 16 MR. CARNEY: Objection. Vague. 17 Deposition testimony? 18 MR. TURNER: All the deposition 19 testimony in the case. 20 A. I think I did. There may have been one or two 21 that I missed, but I certainly reviewed quite a few 22 depositions. 23 Q. So when you see a reference to risk acceptance 24 forms in the testimony, you wanted to see those 25 documents. Is that what happened?</p> <p>43</p>
<p>1 Q. So why were you looking at those documents if 2 that's not part of your assignment? 3 A. My assignment was to look at the assertions -- 4 look at the security statement, analyze the assertions, 5 and compare that with the state of cybersecurity as 6 revealed in the internal documents. 7 Q. Okay. So it -- it doesn't matter whether the 8 internal document is a communication like an e-mail or 9 something like a SARF, right? All of those documents 10 are potentially relevant to whether SolarWinds did the 11 things in the security statement? 12 A. I wouldn't say it didn't matter what they were, 13 but certainly there were things I wanted to consider. I 14 wanted to consider all of the reports, any document that 15 would indicate to me how they actually performed in 16 these areas that I was asked to look at. 17 Q. Right. You would want to consider anything 18 relevant to whether SolarWinds did what was said in the 19 security statement regardless of whether there was an 20 internal communication, presentation, or assessment, 21 fair? 22 A. Well, I -- I knew I couldn't look at absolutely 23 everything because there were hundreds of thousands of 24 documents or more, but what I was looking for was the 25 best picture I could find of what actually was happening</p> <p>42</p>	<p>1 A. When I learned that there were risk assessment 2 forms, and I don't remember exactly how I learned, but 3 when I did, I certainly said, Let's see some of those, 4 let's see those, and we -- I looked at a lot of them. 5 Q. And why did you think risk acceptance forms 6 were relevant? What did they have to do with the 7 security statement? 8 A. Well, there's two or three different ways that 9 they're relevant. For one thing, a risk assessment form 10 is part of software development life cycle. I'm sure 11 we'll talk more about the so-called SDL. So the risk 12 assessment forms are a way of an executive accepting 13 risk on behalf of the company after it's been described 14 in one of these forms. So that's one way. It was very 15 important to understand that. But another -- as it 16 relates to the SDLC. 17 But another important factor, reason to look at 18 the risk acceptance forms, RAF, is because it shows me 19 -- gives me pictures, a depiction of the problems they 20 identified internally with regard to access controls or 21 passwords. And so if they -- the internal engineers, 22 the software developers, or the security people found a 23 problem with access control, and they did, one of the 24 ways they would respond to that was to put together a 25 risk acceptance form.</p> <p>44</p>

Mark Graff
2/14/2025

<p>1 such-and-such a time."</p> <p>2 So that indicates to me that, in many cases,</p> <p>3 they followed a process of filing a request form,</p> <p>4 passing it along, somebody else saw it, acted upon it,</p> <p>5 acknowledged it, made a record, passed it back. That's</p> <p>6 good. When they did that, that's good, and that's a</p> <p>7 process that I've seen before.</p> <p>8 The problem is, and what I found in the report</p> <p>9 and what I called out as an inconsistency, is that the</p> <p>10 mere fact that these forms were being filled out, moved</p> <p>11 around, in many cases acted upon and acted upon</p> <p>12 successfully in many cases; that, by itself, does not,</p> <p>13 in my opinion, based on my experience and my reading of</p> <p>14 all this, that by itself does not mean that they</p> <p>15 consistently adhered to the assertions in the security</p> <p>16 statement about access control.</p> <p>17 MR. TURNER: Okay. I have a few more</p> <p>18 question about this, and then we'll break.</p> <p>19 A. And authentication.</p> <p>20 Q. When you're saying that the forms reflected</p> <p>21 that in many cases things were done successfully, what</p> <p>22 was being done exactly is having an employee get access</p> <p>23 to systems based on their role, right? That was the</p> <p>24 purpose of the form. So you're saying the forms</p> <p>25 demonstrated in many cases that was successfully done?</p> <p>53</p>	<p>1 For example, relating to the MSP product line where they</p> <p>2 had -- talk about access control. They had -- they said</p> <p>3 in their e-mails and reports that there were SolarWinds</p> <p>4 employees who had inappropriate access to customer data.</p> <p>5 Q. Right.</p> <p>6 A. That was a very, very, serious problem and to</p> <p>7 me -- to my mind, yes, in some of these cases that</p> <p>8 reflects systemic issues.</p> <p>9 MR. TURNER: Okay. We can stop there.</p> <p>10 MR. CARNEY: All right, thanks.</p> <p>11 THE VIDEOGRAPHER: The time right now</p> <p>12 is 10:53 a.m., and we are off the record.</p> <p>13 (Whereupon, a short break was taken.)</p> <p>14 THE VIDEOGRAPHER: Stand by, please.</p> <p>15 The time right now is 11:11 a.m., and we're</p> <p>16 back on the record.</p> <p>17 Q. Mr. Graff, could you turn to your rebuttal</p> <p>18 report at page 7, paragraph 15.</p> <p>19 A. I'm there.</p> <p>20 Q. Okay. And you say in -- toward the bottom of</p> <p>21 this paragraph, second to last sentence:</p> <p>22 "My opening report never stated</p> <p>23 anything about the frequency of an issue. As I</p> <p>24 explained in my opening report, the types of</p> <p>25 major issues that slipped through SolarWinds'</p> <p>55</p>
<p>1 MR. CARNEY: Objection to form.</p> <p>2 A. I saw several forms that seemed to indicate</p> <p>3 that somebody, maybe a hiring manager, asked for an</p> <p>4 account to be created for a person coming onboard and</p> <p>5 explained what systems or what data they were to be</p> <p>6 given access to. I saw -- then, sometimes I saw a few</p> <p>7 forms that said, "Yes, I did it. Here's the stuff I</p> <p>8 gave them access to."</p> <p>9 I did see some forms like that, and I think</p> <p>10 probably there were cases when the system worked that</p> <p>11 way and worked successfully.</p> <p>12 Q. Right. And what I'm just trying to get clear</p> <p>13 on, Mr. Graff, is I think what you're saying -- correct</p> <p>14 me if I'm wrong -- but I think what you're saying is,</p> <p>15 even if you saw many instances like that, you considered</p> <p>16 it to be outweighed by the specific examples you cite in</p> <p>17 your report of what you considered to be major issues?</p> <p>18 MR. CARNEY: Objection. Vague.</p> <p>19 A. Yes, if we're talking about, for example,</p> <p>20 access control, if somebody -- if I see a form or I see</p> <p>21 another form or I see a dozen forms where somebody asked</p> <p>22 for an account to be created and specified the data that</p> <p>23 that they should have access to, that's a good thing.</p> <p>24 But it doesn't begin to compensate for the remarkable</p> <p>25 problems that were described by SolarWinds's employees.</p> <p>54</p>	<p>1 internal controls need not materialize many</p> <p>2 times for them to indicate a systemic problem."</p> <p>3 So you are not making a claim about the</p> <p>4 frequency with which SolarWinds followed the practices</p> <p>5 in the security statement; is that right?</p> <p>6 MR. CARNEY: Objection to form.</p> <p>7 A. Could you say that a different way for me?</p> <p>8 Q. You say in the opening report -- excuse me --</p> <p>9 you say here in the rebuttal report --</p> <p>10 A. Yeah.</p> <p>11 Q. -- that "My opening report never stated</p> <p>12 anything about the frequency of an issue."</p> <p>13 So, for example, with respect to role-based</p> <p>14 access controls, you weren't asserting anything about</p> <p>15 the frequency with which SolarWinds implemented</p> <p>16 role-based access controls in the manner described in</p> <p>17 the security statement?</p> <p>18 MR. CARNEY: Objection to form.</p> <p>19 A. Yeah, I think that's right.</p> <p>20 Q. I think as you -- I think this basically gets</p> <p>21 back to what we were discussing before the break. You</p> <p>22 instead were looking for whether there were major issues</p> <p>23 that you considered to be major departures from what was</p> <p>24 described in the security statement; is that right?</p> <p>25 MR. CARNEY: Objection -- objection to</p> <p>56</p>

Mark Graff
2/14/2025

<p>1 form.</p> <p>2 A. Well, that's one of the things. I mean, what I</p> <p>3 was looking for. I was looking for information to help</p> <p>4 me evaluate whether or not the performance in the areas</p> <p>5 we talked about was consistent with the security</p> <p>6 statements. That's what I was looking for. But in</p> <p>7 terms of frequency, yes, I wasn't particularly</p> <p>8 interested in or searching for any kind of frequency.</p> <p>9 My feeling was that if there were significant -- my</p> <p>10 opinion, there's significant issues, very, very,</p> <p>11 important issues that identified by the SolarWinds</p> <p>12 employees themselves as being major security issues and</p> <p>13 so forth, there were a great many of those. And so that</p> <p>14 was sufficient for me to draw a conclusion about there</p> <p>15 being significant issues or significant deviations.</p> <p>16 Q. So I want to be really clear, though. You just</p> <p>17 mentioned "many." You're not saying anything about the</p> <p>18 frequency of problems that arose at SolarWinds; you're</p> <p>19 basically saying you identified a number of issues in</p> <p>20 the report that you considered to be major deviations</p> <p>21 from those practices. And based on those, it's not</p> <p>22 important to you how frequently they complied with these</p> <p>23 practices, given the seriousness of the deviations that</p> <p>24 you saw?</p> <p>25 MR. CARNEY: Objection. Compound.</p> <p>57</p>	<p>1 need not materialize many times for them to</p> <p>2 indicate a systemic problem."</p> <p>3 I want to focus on the word "systemic," because</p> <p>4 my understanding from what you're saying here, by</p> <p>5 "systemic," you don't mean frequent, right? You're not</p> <p>6 saying anything about the frequency of the problem.</p> <p>7 MR. CARNEY: Objection to form.</p> <p>8 Compound.</p> <p>9 A. It's a little more complicated than that.</p> <p>10 There were security issues that were identified as very</p> <p>11 serious that persisted for a very long time, for months</p> <p>12 or for years without being remediated. So you can look</p> <p>13 at that -- you can say that that's only one instance and</p> <p>14 it went on for years, so maybe you only count that once,</p> <p>15 maybe you could count it as being a problem every day,</p> <p>16 but I wasn't talking about the number of times something</p> <p>17 happened. I'm not trying to count those up and</p> <p>18 calculate a percentage or some kind of failure rate.</p> <p>19 What I was saying is that these problems, many</p> <p>20 of which persisted for years, showed a systemic issue in</p> <p>21 the way they were approaching the problems.</p> <p>22 Q. What specific issue persisted for years,</p> <p>23 Mr. Graff? Let's take the MSP example. Are you</p> <p>24 alleging that persisted for years?</p> <p>25 MR. CARNEY: Objection. Compound.</p> <p>59</p>
<p>1 Q. Is that a fair characterization of your</p> <p>2 opinion?</p> <p>3 A. No, I wouldn't put it quite that way. But I</p> <p>4 will say that, as I said before, there are several</p> <p>5 indications from these SARFs, these forms, that there</p> <p>6 was a practice in place, and they did it correctly many</p> <p>7 times, so I -- so I wasn't making an assertion about how</p> <p>8 frequently they failed to do it, but, rather, that there</p> <p>9 were significant occurrences that were flaws and</p> <p>10 mistakes and that these very significant things pointed</p> <p>11 out -- by the way, it wasn't that I found them, the</p> <p>12 SolarWinds employees found them and pointed them out.</p> <p>13 Q. I'm sorry. I missed that. Who pointed them</p> <p>14 out?</p> <p>15 A. It was the SolarWinds employees that -- and</p> <p>16 consultants and I think there were also some external</p> <p>17 researchers that pointed out problems, too. But it</p> <p>18 wasn't me finding the problems. I found the discussions</p> <p>19 in the internal documentation.</p> <p>20 Q. Okay. So let's go back to that last sentence</p> <p>21 in paragraph 15.</p> <p>22 A. Mm-hmm.</p> <p>23 Q. You say:</p> <p>24 "The types of major issue that is</p> <p>25 slipped through SolarWinds' internal controls</p> <p>58</p>	<p>1 Q. Once it was identified?</p> <p>2 A. There's more than one MSP problem, but what I</p> <p>3 had in mind there, was I think it was reported it was</p> <p>4 remediated in five months. But if you look at the --</p> <p>5 what I think is a very serious problem, which is the</p> <p>6 fact that there was a connection between the software</p> <p>7 development environment and the production environment,</p> <p>8 that was reported by -- I think maybe it was Chris Day</p> <p>9 who said that it had been going for years.</p> <p>10 Q. Okay. So let me go back to another statement</p> <p>11 you made and you referred to earlier that perfection</p> <p>12 isn't the standard here, right? Issues arise from time</p> <p>13 to time in any cybersecurity program?</p> <p>14 A. I agree that.</p> <p>15 Q. But basically, are you say if a major issue</p> <p>16 arises from time to time, then you would consider that</p> <p>17 to be, I think as you put it, an indication of a</p> <p>18 systemic problem?</p> <p>19 A. Well, that's kind of a hypothetical. It would</p> <p>20 depend on how it occurred and how big a problem it was</p> <p>21 and whether there was a policy against it and did</p> <p>22 somebody mess up in a simple technical way or was there</p> <p>23 a design problem, which I've seen some of here.</p> <p>24 Q. Sir, I'm trying to -- just before we get into</p> <p>25 the details of the evidence, I want to understand your</p> <p>60</p>

Mark Graff
2/14/2025

<p>1 methodology.</p> <p>2 So again, issues can arise from time to time.</p> <p>3 That doesn't indicate a lack of controls, right?</p> <p>4 A. Well, it could indicate a lack of controls.</p> <p>5 But there -- but perfection is not the standard I was</p> <p>6 applying.</p> <p>7 Q. We can just be specific. If you want to look</p> <p>8 back at your initial report, paragraph 50.</p> <p>9 A. 5-0?</p> <p>10 Q. 5-0. It's on page 25.</p> <p>11 A. All right, I see it.</p> <p>12 Q. You say:</p> <p>13 "My decades of experience have taught</p> <p>14 me that no organization has perfect security</p> <p>15 and that any organization diligently assessing</p> <p>16 its cybersecurity will uncover, from time to</p> <p>17 time, some issues needing to be addressed."</p> <p>18 Right?</p> <p>19 A. Yes.</p> <p>20 Q. So that means that if issues arise from time to</p> <p>21 time, that doesn't mean there's a pervasive failure to</p> <p>22 implement controls?</p> <p>23 A. The mere fact that occasionally a problem</p> <p>24 occurs, that doesn't by itself indicate that there's a</p> <p>25 systemic issue. There are other ways we can identify a</p> <p style="text-align: center;">61</p>	<p>1 Is that essentially your finding?</p> <p>2 MR. CARNEY: Objection to form.</p> <p>3 A. Well, no, I didn't say that they lacked the</p> <p>4 security controls. What I said was that if you look at</p> <p>5 the categorical statements they make about "We apply</p> <p>6 this to all software we develop," and so forth -- I can</p> <p>7 find the exact quote for you -- when they say that, if</p> <p>8 they say they do it for all and you find that the</p> <p>9 employees themselves are pointing out one instance after</p> <p>10 another when they don't do it, then that can be an</p> <p>11 indication of a significant discrepancy between what</p> <p>12 they're doing and what they say they're doing.</p> <p>13 Q. So let's try to be specific. Let's take access</p> <p>14 controls.</p> <p>15 (Discussion off the record.)</p> <p>16 (Whereupon, SolarWinds Security</p> <p>17 Statement was marked as Graff Exhibit 3, for</p> <p>18 identification, as of this date.)</p> <p>19 Q. So if you turn to page 4 of this document,</p> <p>20 under access controls.</p> <p>21 A. Yes, I see it.</p> <p>22 Q. It says: "Role-based access controls are</p> <p>23 implemented for access to information systems."</p> <p>24 Let's just stick with that for a minute. Is</p> <p>25 that a categorical statement, in your view?</p> <p style="text-align: center;">63</p>
<p>1 potential systemic issue.</p> <p>2 Q. But it's your position that if -- what you deem</p> <p>3 a major issue arises, then that does indicate the lack</p> <p>4 of controls?</p> <p>5 A. A significant issue or potentially catastrophic</p> <p>6 incident, some of the ones we've talked about here, no,</p> <p>7 it can indicate a systemic issue. The way I looked at</p> <p>8 these reports of so many problems, I did develop the</p> <p>9 opinion that in some cases, they represented systemic</p> <p>10 issues.</p> <p>11 Q. You keep on saying "so many," and I hate to</p> <p>12 harp on this, Mr. Graff, but you've already said you're</p> <p>13 not making a finding about the frequency of an issue.</p> <p>14 So let's put the "many" aside, because you've said that</p> <p>15 what really matters is the significance of the incidents</p> <p>16 you're looking at.</p> <p>17 So what I'm asking, sir, is if an organization</p> <p>18 can have controls in place and issues arise from time to</p> <p>19 time, I think there's no contradiction in that. I'm</p> <p>20 trying to understand what standard you're ultimately</p> <p>21 applying to determine that SolarWinds did lack the</p> <p>22 controls in the security statement, and what I hear you</p> <p>23 to be saying is that the basis for your opinion that it</p> <p>24 lacked the controls in the security statement is that</p> <p>25 there were major lapses in those controls.</p> <p style="text-align: center;">62</p>	<p>1 A. It says they're implemented, so sure, to that</p> <p>2 extent, they're implying that it's done, yeah.</p> <p>3 Q. What categorical language do you see in that</p> <p>4 statement?</p> <p>5 A. "Are implemented," but it's a pretty ordinary</p> <p>6 statement. They're telling us that they have role-based</p> <p>7 access controls for accessed information systems.</p> <p>8 Q. Yeah. It doesn't say "all information</p> <p>9 systems," right?</p> <p>10 A. It doesn't.</p> <p>11 Q. It doesn't say "always"? None of those words</p> <p>12 that you pointed to earlier, it doesn't contain those</p> <p>13 words, does it?</p> <p>14 MR. CARNEY: Objection. Compound.</p> <p>15 A. The word "all" doesn't appear here, and it</p> <p>16 doesn't say "always." It just says it's done.</p> <p>17 Q. Okay. Let me just go back.</p> <p>18 Is this what you consider a categorical</p> <p>19 statement or not?</p> <p>20 MR. CARNEY: Objection. Vague.</p> <p>21 A. Yeah, there are no qualifications in it. Yeah,</p> <p>22 it says that they do it. It says they are implemented.</p> <p>23 Q. And, again, perfection is not the standard,</p> <p>24 right? So if role-based access controls are implemented</p> <p>25 for access information systems generally, but issues</p> <p style="text-align: center;">64</p>

Mark Graff
2/14/2025

<p>1 arise from time to time, it still means that you would 2 agree with that statement? 3 A. Well, they say role-based access controls are 4 implemented, and there are processes in place to address 5 employees and so forth, there are -- it talks in the 6 second sentence about processes or procedures in place 7 to address employees who are voluntarily or 8 involuntarily terminated, the internal reports show 9 that, in fact, there are problems there. 10 Q. Well, Mr. Graff, if you could just stick with 11 my question. 12 A. Sure. 13 Q. Okay. My question is: If the company had a 14 general practice of implementing role-based access 15 controls to information systems but issues arose from 16 time to time, they weren't perfect, right? You would 17 agree that that statement would still be true? 18 A. I saw in the -- 19 Q. I'm not asking you what you saw, sir. I'm 20 asking you to assume that role-based access controls 21 were implemented for access to information systems, but 22 issues arose from time to time. 23 Would you still agree that the statement is 24 true? 25 MR. CARNEY: Objection. Vague as to</p> <p>65</p>	<p>1 looking at how widespread; in other words, how frequent 2 they were? 3 A. Well, there's a different between widespread 4 and frequent. If it's across all of their systems, if 5 there's a problem across all of their systems, it's a 6 problem that affects all of their data, that's one of 7 the ways I would think it could be widespread. I'm not 8 talking about necessarily the frequency of which it 9 occurs or how often it is, but does it affect all of 10 their systems, does it affect all of their data or much 11 of the customer data? That would make it widespread. 12 Q. Again, I just want to get clear. So 13 essentially, if they had issues arise from time to time 14 by itself, that wouldn't make the statement false, but 15 if there were a major issue in -- if it were an issue 16 you considered major, that would render the statement 17 false; is that the standard you're applying? 18 MR. CARNEY: Objection. Objection. 19 Vague and compound. 20 Q. Whether there was a major issue that you 21 identified in the control being looked at? 22 A. Well, I've use the word "major." I'm not going 23 to restrict myself to that, because I also mentioned 24 that there -- I considered whether or not there were 25 significant exceptions or, as I said, potentially</p> <p>67</p>
<p>1 "issues." 2 A. This asserts that they have access controls are 3 implemented on the basis of roles. I saw some 4 indications that they did that. I also saw some 5 indications that they hadn't done that. 6 Q. So what I'm trying to get at -- I don't care 7 what you saw at this point. I am asking -- I am trying 8 to get clear on the standard you're applying. 9 So assume, again, that the evidence shows that 10 role-based access controls were generally implemented, 11 but there were issues identified from time to time, you 12 would agree that the fact that there were issues 13 identified from time to time does not by itself render 14 that statement false? 15 MR. CARNEY: Objection. Vague. 16 A. It's going to matter what the issues are and 17 how pervasive they were. 18 Q. How pervasive they were? Meaning how 19 widespread they were? 20 A. Yes. For example, role-based access controls 21 were violated -- that principle was violated -- one 22 example that come to mind is the problem with the MSP 23 product line, and so forth, so that was a failure of 24 access controls, among other kinds of controls. 25 Q. I just asked, Mr. Graff, whether you were</p> <p>66</p>	<p>1 catastrophic exceptions. So in order to evaluate 2 whether or not role-based access controls were in place 3 in a manner that was consistent with this security 4 statement, I took a look at what I could find out about, 5 how often, yes, they did it, and I think they created 6 the accounts with these SARFs, they did that often, they 7 did it correctly. 8 Q. They complied, in other words, often correctly? 9 A. Many times with the SARFs. They did that many 10 times with account creation. Now, mind you, they also 11 violated many times when it comes -- when we talked 12 about shared access to account IDs and so forth, right. 13 So there's violations there also, but in terms 14 of role-based access control, they clearly had a system 15 in place where somebody would request it. Whether it 16 was implemented correctly, I can't know, but I think 17 they did very often, they would have complied with the 18 role-based access controls in terms of account creation. 19 There were many problems in other areas as it relates to 20 access controls, and they were significant. We can use 21 the word "major." They were very important. 22 Q. Let me stop you there, Mr. Graff -- 23 A. Yeah, sure. 24 Q. -- because -- and, look, the day will go much 25 quicker if you just stick to answering the specific</p> <p>68</p>

<p>1 question I'm asking you, okay?</p> <p>2 So you used several words in that last answer.</p> <p>3 You said "major," you said "significant," you said</p> <p>4 "catastrophic." I'm trying to understand what your</p> <p>5 threshold is. Is the idea that if there's a significant</p> <p>6 problem that SolarWinds identifies in its access</p> <p>7 controls at some point then that renders this statement</p> <p>8 false, or is it if they identify a major problem or a</p> <p>9 catastrophic problem? What is the standard you're</p> <p>10 applying?</p> <p>11 MR. CARNEY: Objection. Vague and</p> <p>12 compound.</p> <p>13 A. It's going to vary from case to case. One of</p> <p>14 the things I'm referring to is the problems that were</p> <p>15 identified with role-based access control in some of the</p> <p>16 testimony and some of the documentation as well where</p> <p>17 the SolarWinds' employees talked about problems with</p> <p>18 role-based access control.</p> <p>19 Q. I understand the facts may vary from case to</p> <p>20 case, but are you applying a different standard from</p> <p>21 case to case?</p> <p>22 What are you looking for in order to determine</p> <p>23 whether this statement is true, role-based access</p> <p>24 controls are implemented for access to information</p> <p>25 systems. You've repeatedly said the company had a</p> <p style="text-align: center;">69</p>	<p>1 information systems?</p> <p>2 MR. CARNEY: Objection. Asked and</p> <p>3 answered.</p> <p>4 A. I do have an opinion, and in order to</p> <p>5 understand my opinion, it's going to be necessary to</p> <p>6 look at a little broader segment than those two</p> <p>7 sentences.</p> <p>8 Q. Do -- do you have an opinion as to whether it's</p> <p>9 true or false --</p> <p>10 MR. CARNEY: Objection --</p> <p>11 Q. It calls for a true-or-false answer. What --</p> <p>12 which is it? Do you believe that it's true or do you</p> <p>13 believe that it's false?</p> <p>14 MR. CARNEY: Objection. Vague as to</p> <p>15 "it."</p> <p>16 Q. The sentence: "Role-based access controls are</p> <p>17 implemented for access to information systems," do you</p> <p>18 have any opinion as to whether that statement was true</p> <p>19 during the time of the relevant period, and I'm asking</p> <p>20 you just for either true or false?</p> <p>21 A. It's inconsistent with what actually happened</p> <p>22 in their actual practices.</p> <p>23 Q. I'm trying to understand what that means, okay?</p> <p>24 I understand you found certain issues or instances where</p> <p>25 you believe SolarWinds deviated from access control best</p> <p style="text-align: center;">71</p>
<p>1 general process for provisioning access, you've claimed</p> <p>2 that there was either a significant problem or a major</p> <p>3 problem or a catastrophic problem and that is at the</p> <p>4 root of your opinion.</p> <p>5 So what is the standard that you're applying to</p> <p>6 determine that this statement was false?</p> <p>7 MR. CARNEY: Objection. Compound.</p> <p>8 Q. Let me just ask you to clarify, is your opinion</p> <p>9 that this statement was false, role-based access</p> <p>10 controls are implemented for access to information</p> <p>11 systems?</p> <p>12 MR. CARNEY: Objection. Compound.</p> <p>13 A. I'm going to refer to my statement here -- to</p> <p>14 my report. What I've said is that what's described in</p> <p>15 the internal documents is not consistent with that</p> <p>16 security statement as it relates to role-based access</p> <p>17 control.</p> <p>18 Q. Meaning that you think this is untrue,</p> <p>19 role-based access controls are implemented for access to</p> <p>20 information systems; you think that statement is untrue?</p> <p>21 A. Well, I point out in the report that there were</p> <p>22 several cases when it wasn't done.</p> <p>23 Q. That's not what I'm asking, sir. Do you have</p> <p>24 an opinion in this case as to whether or not SolarWinds</p> <p>25 implemented role-based access controls for access to its</p> <p style="text-align: center;">70</p>	<p>1 practices.</p> <p>2 Based on those instances, do you have an</p> <p>3 opinion as to whether this statement is true?</p> <p>4 A. Well, you keep saying I found certain issues.</p> <p>5 I -- it was the SolarWinds people and the customers and</p> <p>6 the external security researchers that found the issues.</p> <p>7 I'm just summarizing them in my report, right, so I</p> <p>8 didn't find them. Let me be clear about that. I didn't</p> <p>9 have access to that information. I couldn't have found</p> <p>10 it.</p> <p>11 Q. I understand that, sir, that's obvious. What</p> <p>12 you said, again, before, is that it's understandable</p> <p>13 that companies from time to time identify issues in</p> <p>14 their cybersecurity controls, right?</p> <p>15 A. Yes. It happens from time to time.</p> <p>16 Q. So what you saw is SolarWinds identifying</p> <p>17 issues related to its controls. So I'm trying to</p> <p>18 understand what the implication of that is for your</p> <p>19 opinion. Based on the issues that you saw, do you</p> <p>20 believe it was false for SolarWinds to say role-based</p> <p>21 access controls are implemented for access for</p> <p>22 information systems? It's a yes-or-no question.</p> <p>23 A. I understand it's a yes-or-no question, but the</p> <p>24 paradigm there I'm saying it's inconsistent. I don't --</p> <p>25 whether it's true or false is a judgment that I didn't</p> <p style="text-align: center;">72</p>

Mark Graff
2/14/2025

<p>1 A. Well, when I was at NASDAQ defending the stock 2 market there, I held them to an extremely high standard, 3 and if I found that they -- what they did didn't match 4 what they told me, I took action. 5 Q. Well let's talk about your time at NASDAQ. So 6 you were with NASDAQ from 2012 to 2015, right? 7 A. Yes, that's right. 8 Q. And NASDAQ had security policies in place while 9 you were there? 10 A. In more than one sense, yes. 11 Q. And you made public statements about those 12 security policies from time to time? 13 A. I made public statements. I don't know if I 14 exactly made statements about our policies. I would 15 have to have my memory refreshed, but it could well be. 16 Q. Do you remember giving testimony before 17 Congress in June 2012? 18 A. Yes, I do. 19 MR. TURNER: Let's take a look at that 20 one. 21 (Whereupon, Testimony of Mark Graff 22 Vice President, NASDAQ OMX Group Before the 23 House Financial Services Committee Subcommittee 24 on Capital Markets was marked as Graff Exhibit 25 4, for identification, as of this date.)</p> <p>77</p>	<p>1 "A summary of processes, policies, and 2 procedures that NASDAQ OMX generally follows in 3 connection with information security." 4 Right? 5 A. Yes. 6 Q. Similar to what you'd see in the security 7 statement is the summary of the various policies that 8 NASDAQ followed. 9 MR. CARNEY: Objection. Vague. 10 Q. And there's a bulleted list under there that 11 includes things like, and I'll just quote: 12 "Business continuity plans are robust 13 in taking into consideration real-time 14 failovers of our market trading platforms and 15 protects against intentional and malicious 16 attempts to disrupt our business." 17 Do you see that one? 18 A. Yes. 19 Q. And there are several bullet like that under 20 it? 21 A. Yes. 22 Q. And all the statements in this testimony were 23 true, right? 24 A. Yes. 25 Q. In fact, this was sworn testimony, so it was</p> <p>79</p>
<p>1 Q. You can take time to thumb through this 2 document, Mr. Graff, but you're being shown what's been 3 marked as Graff Exhibit 4. 4 Do you recognize this as a copy of the 5 testimony you gave to Congress on June 1st, 2012? 6 A. Yes, this looks right. 7 Q. And if you could turn to the second page for 8 me. In the first full paragraph of the second page, you 9 give a general overview of the security program that 10 NASDAQ had in place. 11 Do you see that? 12 A. Well, I'm not sure I would say it was a general 13 overview, but I certainly discuss our defenses. 14 Q. Right. Defenses including: 15 "Implementation of physical safeguards 16 around data centers and work spaces, a 17 consolidated network with multiple connectivity 18 options, a disaster recovery plan for our 19 infrastructure, capacity management and 20 testing, and business continuity and crisis 21 management plans." 22 Those are all components of NASDAQ's security 23 program, right? 24 A. Yes. 25 Q. And then a bit below that, you provide:</p> <p>78</p>	<p>1 given under oath? 2 A. It was. 3 Q. For example, it was true that NASDAQ had: 4 "Robust business continuity plans in place"? 5 A. Yes. 6 Q. And they took into considerations real-time 7 failovers of market trading platforms? 8 A. Yes. And by the way, I can answer some 9 questions about NASDAQ security operations, and others I 10 won't be able to answer for you, but I'll do my best. 11 Q. Sure. Now, business continuity plans are plans 12 that allow an organization to continue operating after 13 technical disruption, right? 14 A. Well, that's the general sense of it. That 15 probably isn't exactly right, but that's the general 16 sense, sure. 17 Q. And so what this is saying if you had robust 18 plans in place to make sure NASDAQ could keep its 19 platforms operating in the event of something like a 20 technical glitch? 21 A. Well, I don't want to get into what a technical 22 glitch is, but we definitely had business continuity 23 plans that were in place to help the system recover, 24 defend against attack, or recover from a -- partially or 25 completely successful attack. We had plans in place.</p> <p>80</p>

1 Q. It could be an attack or it could be an
2 accident or a glitch, or anything; you had robust plans
3 in place to make sure the platform stayed operational?
4 A. We did have -- I can agree with that last part.
5 We did have robust plans in place to make sure that the
6 platforms remain operational.
7 Q. And failovers, that's when computers
8 automatically switch to backup systems when a main
9 system fails, right?
10 A. Yes.
11 Q. So NASDAQ had systems designed to failover at a
12 backup systems in real time?
13 A. Yes.
14 Q. And that's part of how you made sure that the
15 trading platform stayed operational and current?
16 A. That's one of the -- that is one of the
17 techniques we used. There were several others.
18 Q. Now, even though NASDAQ had these policies, it
19 was also true that NASDAQ had gaps in these policies
20 that arose from time to time, right?
21 MR. CARNEY: Objection. Vague.
22 A. I'm having a little trouble with -- with
23 describing all these things as policies.
24 Q. Whatever; practices, policies, there were gaps
25 from time to time, correct?

81

1 MR. CARNEY: Objection. Vague.
2 A. Well, I'm trying to think. We had -- we were
3 very, very successful. Are you asking about gaps that
4 affected operations?
5 Q. I'm asking about any gaps. Every cybersecurity
6 program have gaps in their controls from time to time,
7 right?
8 A. Well, gaps, lapses, maybe. I'm trying to
9 figure out what you mean. We -- we had marvelous
10 results, and I'm trying to think if there were any
11 operational issues.
12 Q. I'm not even talking necessarily about
13 operational issues, but risks that were identified from
14 time to time that you needed to address, right? Every
15 cybersecurity program has that?
16 A. Well, there were certainly risks, depending on
17 how we're going to define the word. I teach a class on
18 this. And I spend -- I'm not going to do it -- I spend
19 all day talking about what the word "risk" means. So --
20 but, yes, we had risks in an ordinary sense, absolutely.
21 We had targeted attacks too.
22 Q. Yeah, Mr. Graff, I'm just going back to your
23 point that no organization has perfect cybersecurity,
24 and every organization will uncover from time to time
25 some issues that need to be addressed.

82

1 So isn't it true that NASDAQ had issues that
2 arose from time to time with respect to, for example,
3 business continuity systems?
4 A. Oh I don't think we had any issues relating to
5 our business continuity issues, but one of the points I
6 --
7 Q. Mr. Graff --
8 A. -- let me --
9 Q. Let me just go into the next question, please.
10 A. I am going to finish my answer.
11 MR. CARNEY: Yes, Serrin, please let
12 him finish.
13 MR. TURNER: I don't need to go off in
14 a different tangent because it's not really
15 relevant in our question.
16 MR. CARNEY: Yeah, but, Serrin, you got
17 to let him finish --
18 MR. TURNER: That's fine. Go ahead and
19 then I'll move to strike as nonresponsive. Go
20 ahead.
21 A. We had -- as I said in my statement before
22 Congress, we had multiple layers of defense. So when
23 you are talking about gaps, I mean, our defenses nestled
24 together to protect the stock market, and we had an
25 extraordinary record of response to attacks. And let me

83

1 distinguish. Of course, we were attacked. We were
2 never successfully attacked, okay. So when you talk
3 about gaps in cybersecurity, we didn't have any gaps in
4 the way we operated our systems and the way we protected
5 the stock market and its data.
6 Q. Let me just ask it a little bit of a different
7 way, Mr. Graff. If there were occasional gaps that
8 arose in your business continuity policies, still
9 wouldn't change the fact that you had robust business
10 continuity programs in place, right?
11 MR. CARNEY: Objection. Vague as to
12 gaps and policies.
13 A. Yeah, I'm afraid --
14 Q. Okay. I'll withdraw the question.
15 How about this: There were major gaps in your
16 business continuity plans at NASDAQ, weren't there,
17 Mr. Graff? Do you remember those?
18 MR. CARNEY: Objection. Vague.
19 A. I -- I need to understand more about what you
20 mean about the gaps, and you are talking about business
21 continuity policies, and there's differences between
22 policies and practices. So I'm afraid I'd like to ask
23 you to be a little more clear in what you're saying.
24 Q. Do you remember, in August 2013, NASDAQ
25 suffered what became known as the flash freeze incident?

84

Mark Graff
2/14/2025

<p>1 Do you remember that?</p> <p>2 A. I think you're talking about the IPO with</p> <p>3 Facebook.</p> <p>4 Q. No. That's a different one. That's in 2012.</p> <p>5 I'm talking about 2013. You don't remember the flash</p> <p>6 freeze?</p> <p>7 A. You'd have to refresh my memory on that.</p> <p>8 Am I going to get a copy of that?</p> <p>9 MR. TURNER: Yes, once it's marked.</p> <p>10 (Whereupon, NASDAQ OMX Provides Updates</p> <p>11 on Events of August 22, 2013 was marked as</p> <p>12 Graff Exhibit 5, for identification, as of this</p> <p>13 date.)</p> <p>14 THE WITNESS: All right. I have it.</p> <p>15 Q. Take a minute to review if you'd like, but this</p> <p>16 is a NASDAQ statement from -- published looks like</p> <p>17 August 29, 2013, titled: "NASDAQ OMX Provides Updates</p> <p>18 on Events of August 22, 2013."</p> <p>19 Does this refresh your recollection at all</p> <p>20 about this event?</p> <p>21 A. I'll need another minute to look.</p> <p>22 Q. Sure.</p> <p>23 A. All right. I've reviewed the document.</p> <p>24 Q. Does this refresh your recollection about the</p> <p>25 incident? Do you remember that trading stopped on</p> <p style="text-align: center;">85</p>	<p>1 A. I do see that.</p> <p>2 Q. And that's what led to the freeze here. Is</p> <p>3 that your understanding?</p> <p>4 A. I don't know. I really didn't get involved in</p> <p>5 this because it wasn't a cybersecurity incident, and I</p> <p>6 had no responsibility for the failover of the</p> <p>7 processors. So I didn't get involved in this.</p> <p>8 Q. Does cybersecurity -- have you ever heard of</p> <p>9 the abbreviation "CIA" in cybersecurity?</p> <p>10 A. Sure.</p> <p>11 Q. Confidentiality, integrity, and availability?</p> <p>12 A. Mm-hmm, yes.</p> <p>13 Q. And cybersecurity protects all three aspects of</p> <p>14 data, right?</p> <p>15 A. Well, I lecture on this too. Cybersecurity</p> <p>16 helps to ensure availability of systems against attack</p> <p>17 or malfeasance or mistakes. But this wasn't a</p> <p>18 cybersecurity incident, and I didn't have the</p> <p>19 responsibility for the uptime of the entire stock</p> <p>20 market.</p> <p>21 Q. You said malfeasance or mistakes?</p> <p>22 A. Uh-huh.</p> <p>23 Q. Isn't a mistake if there's a flaw in the code</p> <p>24 that causes the exchange to go down?</p> <p>25 A. I suppose there was a mistake. I wasn't</p> <p style="text-align: center;">87</p>
<p>1 NASDAQ for more than three hours?</p> <p>2 A. I wouldn't have been able to tell you that. I</p> <p>3 see it says that here.</p> <p>4 Q. And according to this document, the cause was a</p> <p>5 spike in trading messages at the NASDAQ that exceeded</p> <p>6 its capacity to process.</p> <p>7 Does that sound right to you?</p> <p>8 A. Yeah.</p> <p>9 Q. And that should have caused a failover to a</p> <p>10 backup system, I believe it says, but there was a flaw</p> <p>11 in NASDAQ's code that prevented the failover from</p> <p>12 happening cleanly?</p> <p>13 MR. CARNEY: Can you direct us --</p> <p>14 MR. TURNER: Yes, one moment.</p> <p>15 MR. CARNEY: Thanks.</p> <p>16 Q. Directing your attention to the middle of</p> <p>17 page 2, starting with:</p> <p>18 "The confluence of these events vastly</p> <p>19 exceeded the SIP's planned capacity, which</p> <p>20 caused its failure and then revealed a latent</p> <p>21 flaw in the SIP's software code. This latent</p> <p>22 flaw prevented the system's built-in redundancy</p> <p>23 capabilities from failing over cleanly, and</p> <p>24 delayed the return of system messages."</p> <p>25 Do you see that?</p> <p style="text-align: center;">86</p>	<p>1 responsible for the operation of the stock market as</p> <p>2 such. I was responsible for protecting them against</p> <p>3 cybersecurity incidents. This wasn't one.</p> <p>4 Q. Business continuity plans, you were in charge</p> <p>5 of those, correct? That's part of the cybersecurity</p> <p>6 program?</p> <p>7 A. We had some business continuity plans. That</p> <p>8 wasn't -- I didn't have responsibility for the business</p> <p>9 continuity plans, that was a whole other department and</p> <p>10 a whole other vice president.</p> <p>11 Q. You testified, however, that the NASDAQ had</p> <p>12 robust business continuity plans. Were you only</p> <p>13 testifying that they were robust against attackers but</p> <p>14 not robust against glitches? Is that how Congress would</p> <p>15 have understood your testimony?</p> <p>16 MR. CARNEY: Objection. Vague.</p> <p>17 Mischaracterizes testimony. You can refer him</p> <p>18 to the testimony itself on page 2.</p> <p>19 Q. Mr. Graff --</p> <p>20 A. I have a lot of pieces of paper in front of me.</p> <p>21 Yes, go ahead.</p> <p>22 MR. CARNEY: I mean, I'm reading the</p> <p>23 statement here: "Below is a summary of the</p> <p>24 process, policies, and procedures that NASDAQ</p> <p>25 OMX generally follows in connection with</p> <p style="text-align: center;">88</p>

Mark Graff
2/14/2025

<p>1 information security."</p> <p>2 MR. TURNER: Yes.</p> <p>3 Q. And part of having business continuity plans in</p> <p>4 place, part of the purpose of having business continuity</p> <p>5 plans is to ensure the continued availability of data?</p> <p>6 A. Yes, that's right.</p> <p>7 Q. Okay. So this was a gap in the company's</p> <p>8 business continuity processes, was it not?</p> <p>9 MR. CARNEY: Objection. Vague as to</p> <p>10 "this."</p> <p>11 A. The -- the incident you are talking about that</p> <p>12 had happened in 2013, the so-called "SIP" problem, yes,</p> <p>13 that would have been a -- there was an outage that</p> <p>14 represents an issue with the provisions that NASDAQ made</p> <p>15 at that time for business continuity.</p> <p>16 (Court reporter clarification.)</p> <p>17 Q. Yeah. And it stemmed from a problem, an issue,</p> <p>18 with NASDAQ's business continuity plans or business</p> <p>19 continuity processes?</p> <p>20 A. Well apparently there was a problem in the</p> <p>21 software where there was a cascade of data coming, I</p> <p>22 think coming from the New York Stock Exchange, and so</p> <p>23 their system wasn't able to keep up with it, and it</p> <p>24 resulted in an outage. Absolutely.</p> <p>25 Q. And that's a gap, right? It wasn't designed to</p> <p style="text-align: center;">89</p>	<p>1 Q. Okay.</p> <p>2 A. And NASDAQ took responsibility for the issues.</p> <p>3 Q. Right. And none of this doesn't mean -- excuse</p> <p>4 me -- none of this means, sir, that your prior testimony</p> <p>5 wasn't true, right?</p> <p>6 A. My testimony in front of Congress was accurate</p> <p>7 and factual.</p> <p>8 Q. NASDAQ did have robust continuity plans in</p> <p>9 place, which included systems designed to failover in</p> <p>10 realtime?</p> <p>11 A. Yes.</p> <p>12 Q. As a general matter, it did?</p> <p>13 A. Yes.</p> <p>14 Q. But that doesn't mean its systems were perfect,</p> <p>15 right?</p> <p>16 A. That's right.</p> <p>17 Q. In fact, it says, toward the end of this</p> <p>18 statement here, on page 3, at the top, it says:</p> <p>19 "NASDAQ OMX is deeply disappointed in</p> <p>20 the events of August 22, and our performance is</p> <p>21 unacceptable to our members, issuers and the</p> <p>22 investing public. While getting to 100 percent</p> <p>23 performance in all of our activities, including</p> <p>24 our technology is difficult, it's our</p> <p>25 objective."</p> <p style="text-align: center;">91</p>
<p>1 deal with that risk?</p> <p>2 MR. CARNEY: Objection. Vague.</p> <p>3 A. Well, I wasn't -- I didn't ever see that</p> <p>4 software. I don't know what it was designed to do.</p> <p>5 Clearly, the business continuity plan didn't operate the</p> <p>6 way it should have.</p> <p>7 Q. And, in fact, there's a statement here -- hang</p> <p>8 on one second. One moment, please. I'm sorry. I was</p> <p>9 looking at the wrong page.</p> <p>10 Page 1. Second paragraph, it says:</p> <p>11 "A preliminary internal review has</p> <p>12 identified a combined series of technology</p> <p>13 events that caused the initial market problems</p> <p>14 and extended the halt period. A number of</p> <p>15 these issues were clearly within the control of</p> <p>16 NASDAQ OMX. As a securities information</p> <p>17 processor for NASDAQ stocks, we are responsible</p> <p>18 for them, regret them and intend to take all</p> <p>19 steps necessary to address them, to enhance</p> <p>20 stability and functionality in the markets."</p> <p>21 So there were issues that were under NASDAQ's</p> <p>22 control related to its business processes that caused</p> <p>23 the incident and that needed to be fixed after the</p> <p>24 incident, right?</p> <p>25 A. Yes, that's what it says. I agree.</p> <p style="text-align: center;">90</p>	<p>1 So in other words, while perfection is the</p> <p>2 ideal, you can't expect it in practice; isn't that</p> <p>3 basically what this statement is saying?</p> <p>4 A. Well, I don't know that I want to paraphrase</p> <p>5 something that was written all these years ago. But</p> <p>6 certainly, I'll agree with the idea that perfection is</p> <p>7 not achievable in every case. There is -- as I said in</p> <p>8 my report, there are -- a company is -- will not have</p> <p>9 perfect cybersecurity and they will. If they're</p> <p>10 searching carefully, they will occasionally encounter an</p> <p>11 issue.</p> <p>12 Q. Yeah. And even if an issue occurs, it doesn't</p> <p>13 mean they had a failure to have practices in place.</p> <p>14 Just like in this case, there was an issue, but</p> <p>15 nonetheless, as you've testified, there were, in fact,</p> <p>16 robust business continuity practices in place?</p> <p>17 A. Are we talking now about the NASDAQ OMX</p> <p>18 incident in 2013?</p> <p>19 Q. Yes. Again, even though this issue arose, you</p> <p>20 truthfully testified there were robust business</p> <p>21 continuity procedures in place? Those two things are</p> <p>22 not incompatible, right?</p> <p>23 A. Well, first of all, my testimony was about a</p> <p>24 year ahead of this incident. And, in fact, my testimony</p> <p>25 was prior to the Facebook problem I talked about, with</p> <p style="text-align: center;">92</p>

Mark Graff
2/14/2025

<p>1 the Facebook IPO.</p> <p>2 But what I said in front of Congress was true.</p> <p>3 We did have the business continuity plans and some</p> <p>4 provisions that I felt were robust. I was reporting, I</p> <p>5 didn't have personal responsibilities or administrative</p> <p>6 responsibilities for those plans, but I reported</p> <p>7 truthfully that we did have business continuity plans.</p> <p>8 And sometime later, both with the Facebook IPO in 2012,</p> <p>9 not too long after I testified --</p> <p>10 Q. The Facebook IPO was in May 2012, sir, before</p> <p>11 you testified.</p> <p>12 A. Was it May? And then before I testified?</p> <p>13 Yeah, that's fine. I agree with you.</p> <p>14 Q. Let me make sure I understand what you agree</p> <p>15 with me on. I just want to get a clear answer for the</p> <p>16 record.</p> <p>17 A. The dates of the Facebook incident, that does</p> <p>18 sounds more accurate, sure.</p> <p>19 Q. Okay. But look, you can have robust continuity</p> <p>20 procedures in place, but nonetheless, issues can arise</p> <p>21 from time to time, fair?</p> <p>22 A. Well, it depends what you mean by "issues." I</p> <p>23 mean, of course, there are going to be imperfections.</p> <p>24 But when we use the broad term "issues," that's a</p> <p>25 different matter altogether.</p> <p>93</p>	<p>1 addressing technological vulnerabilities of</p> <p>2 exchanges and other market participants."</p> <p>3 So you would agree that this was a major issue</p> <p>4 that arose for NASDAQ?</p> <p>5 MR. CARNEY: Objection. Vague.</p> <p>6 Q. It was a major issue in connection with</p> <p>7 NASDAQ's business continuity controls?</p> <p>8 MR. CARNEY: Are you saying</p> <p>9 cybersecurity? Are you tying it to</p> <p>10 cybersecurity? That's why it's vague.</p> <p>11 MR. TURNER: I don't need the speaking</p> <p>12 objection.</p> <p>13 Go ahead, Mr. Graff.</p> <p>14 A. Well, this statement relates to an outage that</p> <p>15 occurred on August 22, 2013, a disruption of trading</p> <p>16 activities as a result of a technical flaw that was</p> <p>17 described in the NASDAQ statement. It had nothing to do</p> <p>18 with cybersecurity. The outage didn't have anything do</p> <p>19 with cybersecurity, and it wasn't part of my</p> <p>20 responsibilities, and I don't remember the incident very</p> <p>21 well, to be honest.</p> <p>22 Q. Mr. Graff, I'm just asking you whether this</p> <p>23 qualifies as a serious issue in connection with NASDAQ's</p> <p>24 business continuity processes?</p> <p>25 MR. CARNEY: Objection. Vague.</p> <p>95</p>
<p>1 Q. Let me ask you, sir, this issue is fairly</p> <p>2 described as a major one, correct?</p> <p>3 A. You're talking about the business outage at</p> <p>4 NASDAQ in 2013?</p> <p>5 Q. Yes. Yes.</p> <p>6 A. Yes, I think we can call that a major incident.</p> <p>7 Q. In fact, the SEC itself put out a statement as</p> <p>8 to this trading disruption.</p> <p>9 (Whereupon, Statement on NASDAQ Trading</p> <p>10 Interruption was marked as Graff Exhibit 6, for</p> <p>11 identification, as of this date.)</p> <p>12 Q. So I'm showing you what's been marked as Graff</p> <p>13 Exhibit 6. It's from August 22, 2013, Statement on</p> <p>14 NASDAQ Trading Interruption by chief -- excuse me, Chair</p> <p>15 Mary Jo White.</p> <p>16 Do you see that?</p> <p>17 A. Oh, I see it, yes.</p> <p>18 Q. And it says:</p> <p>19 "The continuous and orderly functioning</p> <p>20 of the securities markets is critically</p> <p>21 important to the health of our financial system</p> <p>22 and the confidence of investors. Today's</p> <p>23 interruption in trading, while resolved before</p> <p>24 the end of the day, was nonetheless serious and</p> <p>25 should reinforce our collective commitment to</p> <p>94</p>	<p>1 Outside the scope.</p> <p>2 A. Well, the disruption was certainly serious.</p> <p>3 The flaw in design that NASDAQ identified was,</p> <p>4 therefore, a serious flaw. You -- I guess, the other</p> <p>5 thing that didn't go right was that the failover doesn't</p> <p>6 seem to have happened as it should have. And so there's</p> <p>7 a -- that's a serious issue as regards to the failovers,</p> <p>8 too.</p> <p>9 Q. Okay. And there's -- this isn't just Mary Jo</p> <p>10 White who had this reaction.</p> <p>11 (Whereupon, news article entitled</p> <p>12 NASDAQ: 'Connectivity issue' Led to Three-Hour</p> <p>13 Shutdown was marked as Graff Exhibit 7, for</p> <p>14 identification, as of this date.)</p> <p>15 Q. So I'm showing you what's been marked as Graff</p> <p>16 Exhibit 7. It's a news article about the shutdown,</p> <p>17 which quotes on page 3 a quote from former SEC Chairman</p> <p>18 Harvey Pitt, saying it looked like NASDAQ was clueless</p> <p>19 about how to deal with this emergency.</p> <p>20 Again, I'm not doing this, Mr. Graff, to</p> <p>21 suggest that you were. But my point is, NASDAQ wasn't</p> <p>22 clueless, it did have business continuity plans in</p> <p>23 place. It's just in this one respect, they failed,</p> <p>24 right?</p> <p>25 A. Well, NASDAQ had robust defenses in -- both in</p> <p>96</p>

Mark Graff
2/14/2025

<p>1 the cyber area and also in other areas, and although 2 this wasn't a cybersecurity incident by any stretch of 3 the imagination, there was an outage that lasted a few 4 hours. It was a serious problem, I agree, and it looks 5 to me, in retrospect, although I really don't remember 6 the incident very well, that the business continuity 7 plans should have handled it better than they did. 8 That's why they apologized. 9 Q. Yeah. And so my only point in all this, 10 Mr. Graff, is just because a major issue arises, that 11 doesn't imply that there was any systemic failure to 12 implement controls, does it? 13 MR. CARNEY: Objection. Vague as to 14 "controls." 15 A. Well, an outage like this -- this one, 16 apparently, according to the statement, came from a 17 design flaw. So we could talk about whether or not, you 18 know, design flaws sometimes indicate a systemic issue, 19 sometimes they don't. But that doesn't really relate to 20 the kinds of failures that I described in my report that 21 were identified by the SolarWinds employees and others, 22 as I've said. 23 Q. Mr. Graff, you told Congress the business 24 continuity plans were robust and took into consideration 25 realtime failovers of market trading platforms. That</p> <p>97</p>	<p>1 A. Significant, you bet. 2 Q. That doesn't mean NASDAQ didn't have business 3 continuity controls in place? 4 A. Yeah, we had controls in place. The controls 5 seemed to have failed for a few hours, but yeah. 6 MR. TURNER: All right. We can take a 7 break now if you want. 8 THE VIDEOGRAPHER: The time right now 9 is 12:08 p.m. We're off the record. 10 (Whereupon, a short break was taken.) 11 THE VIDEOGRAPHER: Stand by, please. 12 The time right now is 1:02 p.m., and we're back 13 on the record. 14 Q. Welcome back, Mr. Graff. 15 A. Thank you. 16 Q. So let's get more specific and talk about some 17 of the particular assertions in the security statement 18 that are at issue. I want to start with the statement 19 following NIST, the statement that SolarWinds follows 20 the NIST cybersecurity framework. 21 You say in paragraph 21 of your report -- you 22 say that this statement was too vague for you to 23 evaluate. 24 Do you remember that? 25 A. I do remember.</p> <p>99</p>
<p>1 was true, right? You had robust continuity plans in 2 place. That does not imply that there might not be 3 serious issues that arise with respect to those 4 controls? 5 MR. CARNEY: Objection to form. 6 A. Well, we -- yeah, I told Congress we had robust 7 business continuity plans. We did. And the system, 8 nevertheless, was overwhelmed and failed for a few hours 9 in 2013. 10 Q. And that doesn't make your testimony false, 11 does it? 12 A. Well, they're not related really. I talked 13 about what our plans were and what our processes were. 14 And I don't believe I said that we would be able to 15 resist any possible problem. 16 Q. Yeah, you didn't say they would be perfect, 17 right? 18 A. I didn't say that. 19 Q. Right. They weren't perfect in this instance, 20 right? 21 A. In the NASDAQ outage instance and the SIP 22 incident. 23 Q. They were not perfect in that instance? 24 A. They were not perfect, I agree. 25 Q. And the consequences were major, right?</p> <p>98</p>	<p>1 Q. So I just want to be clear. You did not try to 2 evaluate whether this assertion was true or false, 3 correct? 4 A. What was that paragraph number? Is it 21, did 5 you say? 6 Q. Paragraph 21 on page 8. 7 A. I did not try to evaluate whether that 8 particular statement was, per se, true or false. 9 Q. So you don't have the opinion that the 10 assertion was false? 11 A. I found that it was not a clear enough 12 statement given the context of the cybersecurity 13 framework to evaluate whether or not they actually were 14 following it. Because it's not clear to me what they 15 mean by "follow" exactly, because it's not a standard. 16 Q. All right. Fair enough. And when you say it's 17 not a standard, you mean it doesn't prescribe specific 18 practices that companies are supposed to follow? 19 A. Well, that's not precisely what I mean. There 20 are cybersecurity standards. There's the ISO/IEC 27001, 21 which is, of course, the European. There are standards 22 in Europe, the GDPR and so forth, but the U.S. doesn't 23 have -- for unclassified systems -- doesn't have a 24 formal standard in cybersecurity. There are 25 recommendations, guidelines, frameworks, but there's not</p> <p>100</p>

1 appropriate to their cases.
 2 **Q.** Exactly. It is a self-assessment framework,
 3 right? It can be used by small businesses and large
 4 businesses alike. They can go through and pick which
 5 controls are appropriate to their situation. It could
 6 be very different for another company.
 7 **MR. CARNEY:** Objection. Compound.
 8 **A.** Could you break that up for me a little bit?
 9 **Q.** And I right that this is a framework -- the
 10 NIST CSF is a framework that is meant for businesses of
 11 all sort to use, no matter how large or small?
 12 **A.** It can be useful for a great many companies, no
 13 matter what their size.
 14 **Q.** And the reason for that is that it's flexible,
 15 like you said; the companies can go through and see
 16 which controls make sense for them and evaluate
 17 themselves against those but ignore others?
 18 **A.** Right. The job -- the framework provides a way
 19 of looking at cybersecurity risks. It suggests how they
 20 can go about it, and it -- they offer -- especially,
 21 there's different versions of the cybersecurity
 22 framework. There's version 1 and version 2. During
 23 this period we're talking about, they only had version
 24 1. But there are a great many controls and ideas that
 25 they will select from.

105

1 **Q.** They will select from but not necessarily meet?
 2 **A.** Well, there are hundreds of possible controls,
 3 so they wouldn't be meeting all of them. The idea is
 4 for them to make a decision based on their assessment of
 5 risks and threats and their business needs and many
 6 other factors.
 7 **Q.** I think you refer to it as a "menu of
 8 recommendations" that the organization can choose from?
 9 **A.** There are -- there are menus. I'm not sure the
 10 framework exactly is a menu. It does provide menus. It
 11 refers to 853, for example, which I'll refer to a lot,
 12 has got lots of these controls they can pick from.
 13 **Q.** Yeah. It's an informative reference, right?
 14 853 is an informative reference? Are you familiar with
 15 that NIST term?
 16 **A.** It doesn't ring a bell, but it is an
 17 informative reference.
 18 **Q.** Yeah, meaning it can inform your application of
 19 the framework, but you're not required to meet all of
 20 those controls listed in 853?
 21 **A.** It's absolutely true that the -- that the
 22 framework does not set up any kind of requirement for
 23 them to adhere to all of the controls in 853.
 24 **Q.** Or any?
 25 **A.** Certainly, there is not a requirement that they

106

1 adhere to any particular one.
 2 **Q.** Okay. So when someone says they're following
 3 the NIST cybersecurity framework, you can't infer from
 4 that that they meet any specific controls?
 5 **A.** I think it would -- yeah, I think you're right.
 6 I think you don't -- from that statement alone, you
 7 can't infer of the hundreds of potential controls which
 8 ones they might be instituting.
 9 **Q.** I can show you this, if you want, but I'm just
 10 reading a NIST publications -- well, I'll show it to
 11 you.
 12 (Whereupon, NIST Cybersecurity
 13 Framework 2.0: Small Business Quick-Start
 14 Guide was marked as Graff Exhibit 8, for
 15 identification, as of this date.)
 16 **Q.** This happens to be a NIST publication for small
 17 businesses, but on the second page, middle paragraph, it
 18 says:
 19 "The NIST cybersecurity framework is
 20 voluntary guidance that helps organizations,
 21 regardless of size, sector or maturity, better
 22 understand, assess, prioritize and communicate
 23 their cybersecurity efforts."
 24 That's an accurate statement, right?
 25 **A.** Yes.

107

1 **Q.** And you don't contest that SolarWinds did use
 2 NIST CSF as a guide to help it better understand,
 3 assess, prioritize and communicate their cybersecurity
 4 efforts, do you?
 5 **A.** Well, I actually haven't seen, that I recall,
 6 any evidence that they used it to -- as a framework for
 7 their cybersecurity designing or cybersecurity program.
 8 I don't think I was really looking at that. I mean,
 9 I -- it's -- they -- I wouldn't be at all surprised if
 10 they consulted it, but I don't know of any evidence that
 11 they based their program on it.
 12 **Q.** You don't recall seeing NIST scorecards among
 13 the evidence that you looked at?
 14 **A.** I did see a NIST scorecard. That's a lot
 15 different than basing a program on it or even basing
 16 your selection of controls.
 17 **Q.** Did you remember the NIST -- excuse me -- the
 18 self-assessments that Mr. Quitugua did that were mapped
 19 to NIST CSF --
 20 **A.** I do recall seeing some of that, mm-hmm.
 21 **Q.** Is that an example of using the NIST framework
 22 to assess yourself?
 23 **MR. CARNEY:** Objection.
 24 **A.** When you say "using the NIST framework," are
 25 you talking specifically about the cybersecurity

108

Mark Graff
2/14/2025

<p>1 A. Yes, I see it.</p> <p>2 Q. It describes how the company had a subscription</p> <p>3 with Palo Alto that they used to globally watch --</p> <p>4 excuse me -- Palo -- strike that.</p> <p>5 Subscription was for a service that's provided</p> <p>6 by Palo Alto where they were watching globally all of</p> <p>7 their firewalls across all of their companies. If they</p> <p>8 saw something suspicious happening in one region, they'd</p> <p>9 send out a heuristical imprint.</p> <p>10 It goes on, and it talks about this is the</p> <p>11 system they used to monitor their firewalls for</p> <p>12 suspicious traffic. Again, isn't that consistent with</p> <p>13 what the security statement says, that high-availability</p> <p>14 firewalls were monitored for the protection and</p> <p>15 prevention of various network security threats?</p> <p>16 A. Well, I'm looking at the quote from Mr. Cline,</p> <p>17 and that, by itself, doesn't necessarily match what we</p> <p>18 were -- what we were just talking about in terms of the</p> <p>19 network security. If I look at Dr. Rattray's summary of</p> <p>20 it, I see that he mentioned some of that, but I don't</p> <p>21 see that in Mr. Cline's testimony.</p> <p>22 Q. Do you see in Mr. Cline's testimony that they</p> <p>23 had Palo Alto firewalls in place?</p> <p>24 A. They may have had many different kinds of</p> <p>25 firewalls. I see that he describes they did have Palo</p> <p style="text-align: center;">141</p>	<p>1 A. If that's what they did, it is evidence in</p> <p>2 support of that contention, you bet.</p> <p>3 Q. And then, in addition, we have the monitoring</p> <p>4 reports which show that reports were generated on a</p> <p>5 daily basis about various types of traffic that might</p> <p>6 indicate threats. Would that also be evidence</p> <p>7 suggesting that the company monitored its firewalls for</p> <p>8 threats?</p> <p>9 A. Well, if he's -- if the reports were the kind</p> <p>10 you showed me were generated and reviewed every day,</p> <p>11 sure, that would be a good practice with regard to</p> <p>12 network monitoring. It wouldn't be, as I said,</p> <p>13 everything you need to do.</p> <p>14 Q. So you don't have any basis to contest that</p> <p>15 SolarWinds monitored its network for security threats?</p> <p>16 A. I really don't have enough information about</p> <p>17 how well they were doing the monitoring --</p> <p>18 Q. That's not the question, sir. I'm not asking</p> <p>19 you about how well.</p> <p>20 A. Mm-hmm.</p> <p>21 Q. The question is: You don't have any basis to</p> <p>22 contest that SolarWinds monitored its network for</p> <p>23 security threats regardless of how well you think it was</p> <p>24 done?</p> <p>25 A. There was some network monitoring that was</p> <p style="text-align: center;">143</p>
<p>1 Alto firewalls and could have had many others in</p> <p>2 different parts of the network.</p> <p>3 Q. Could you just answer my question, please. My</p> <p>4 question was: Do you see in Mr. Cline's testimony</p> <p>5 describes that they had Palo Alto firewalls in place?</p> <p>6 Do you see that?</p> <p>7 A. It says they have subscription with Palo Alto</p> <p>8 with what was called Wildfire.</p> <p>9 Q. Mm-hmm.</p> <p>10 A. It doesn't actually exclusively say, but I'm --</p> <p>11 they do have -- I'm sure they did have Palo Alto</p> <p>12 firewalls.</p> <p>13 Q. And it describes the subservice that they had</p> <p>14 through Palo Alto to monitor those firewalls for</p> <p>15 threats?</p> <p>16 A. Yes, I see that in the second paragraph.</p> <p>17 Q. And then if you take a look at the next page,</p> <p>18 there's testimony from Mr. Brown saying:</p> <p>19 "One of the things the InfoSec team did</p> <p>20 was look at all the events and alerts that came</p> <p>21 through firewalls to say is there anything</p> <p>22 suspect that I should look at here, anything</p> <p>23 suspect here that I should review."</p> <p>24 Again, is that not evidence that the firewalls</p> <p>25 were monitored for threats?</p> <p style="text-align: center;">142</p>	<p>1 being done, absolutely. There was a lot of it, from the</p> <p>2 appearances of it.</p> <p>3 Q. And yet you did not credit that evidence in</p> <p>4 order to find that the statement in the security</p> <p>5 statement about network monitoring was true, did you?</p> <p>6 MR. CARNEY: Objection.</p> <p>7 Mischaracterizes testimony.</p> <p>8 A. I didn't reach a conclusion, for the reasons I</p> <p>9 think I mentioned.</p> <p>10 Q. So where you see evidence of compliance with</p> <p>11 something in the security statement, that's not</p> <p>12 sufficient for you to conclude that the practice was</p> <p>13 done, but when you see evidence for some problem, you</p> <p>14 conclude from that that the practice was not followed.</p> <p>15 Is that a fair summary of your methodology?</p> <p>16 MR. CARNEY: Objection. Argumentative</p> <p>17 and mischaracterizes the testimony.</p> <p>18 Q. So let me put this differently, then,</p> <p>19 Mr. Graff. If you have no basis to contest that network</p> <p>20 monitoring was done, if you've seen evidence that it was</p> <p>21 done, why are you not able to form an opinion as to</p> <p>22 whether this statement in the security statement was</p> <p>23 true?</p> <p>24 MR. CARNEY: Objection. Vague as to</p> <p>25 "this statement".</p> <p style="text-align: center;">144</p>

Mark Graff
2/14/2025

<p>1 A. Well, first of all, what I want to do right now 2 is go back to my final conclusion with regard to network 3 monitoring and explain that, and then I'll be as 4 responsive as I possibly can be to your question. 5 Summary of Opinions, page 8. If anybody can 6 help me find that specific reference to network 7 monitoring in my conclusion, I'd take the help. 8 MR. BRUCKMANN: I believe it's in 9 paragraph 24, Mark. 10 THE WITNESS: And I'm looking at 28, 11 but let me see paragraph 24. 12 A. Yep. So I said here: 13 "I found insufficient evidence to 14 evaluate the network monitoring practices or to 15 evaluate whether they were aware of any 16 deficiencies." 17 Now, certainly, the Palo Alto network reports 18 that you showed me, and I know there were a great many 19 of them, if they were done daily and done well, that's 20 great. That would be an example of network monitoring. 21 If they've got a service from Palo Alto networks that 22 looks for anomalies, that's good, and that would 23 constitute some kind of network monitoring. 24 What I wasn't able to do was to -- what I didn't do as 25 part of this assignment was to evaluate the extent to</p> <p>145</p>	<p>1 "SolarWinds documented numerous issues 2 with network monitoring over the years and that 3 the documents reflected 'many critical network 4 monitoring failures.'" 5 Did you see any documentation like that in your 6 review? 7 MR. CARNEY: Objection. Vague. 8 A. Did I see any documents that indicated -- 9 Q. That there were -- I'll read it to you again: 10 "SolarWinds documented numerous issues 11 with network monitoring over the years and the 12 documents reflected many critical networking 13 failures." 14 Did the SEC provide you with documentation like 15 that? 16 A. That's a complicated question. I'm going to 17 take a moment to think about it. 18 One of the things that your question asks is -- 19 or brings to my mind is how would you know if a document 20 showed a network monitoring problem? All right. So you 21 can look at logs that show the activity. How would you 22 determine whether or not there are deficiencies or 23 problems with network monitoring? 24 Q. Mr. Graff, if you had been presented with 25 documents reflecting numerous issues with network</p> <p>147</p>
<p>1 which what actually happened in terms of network 2 monitoring, and there was some being done, no question, 3 and some I'm pretty confident, it looks like. What I 4 didn't do is reach an opinion as to whether that matched 5 what was described in the security statement. 6 Q. And, again, what it says in the security 7 statement is simply: 8 "Our firewalls are monitored for the 9 detection and prevention of various network 10 security threats." 11 MR. CARNEY: Objection. 12 Mischaracterizes the security statement. 13 Q. I'll read it in full. 14 "Our infrastructure servers reside 15 behind high-availability firewalls and are 16 monitored for the detection and prevention of 17 various network security threats." 18 MR. CARNEY: There's an entire 19 paragraph -- or three paragraphs under network 20 security. 21 MR. TURNER: That's the sentence I'm 22 asking about. 23 Q. Let me put it to you differently, Mr. Graff. 24 Are you aware that the SEC in this case has alleged, 25 quote:</p> <p>146</p>	<p>1 monitoring over the years, wouldn't you have said 2 something about that in your report? 3 Did you or did you not see documents reflecting 4 numerous issues with network monitoring over the years 5 in the evidence you reviewed? 6 A. Well, I'm trying to -- I'm trying to figure out 7 what would constitute that kind of evidence and whether 8 I saw any of it. 9 Q. Can I refer you back to paragraph 24 of your 10 report? 11 A. Sure. 12 Q. Where you say: 13 "Within the documents that I have 14 reviewed, I found insufficient evidence either 15 to evaluate SolarWinds' network monitoring 16 practices or to evaluate whether SolarWinds' 17 personnel were aware of any deficiencies in 18 this area," underscored, and says, "that 19 related assertions in the security statement." 20 A. Right. 21 Q. So can I get a plain answer to my question, 22 sir? Did you see any documents documenting many 23 critical network monitoring failures at SolarWinds? Yes 24 or no? 25 A. Well, I didn't see any --</p> <p>148</p>

Mark Graff
2/14/2025

<p>1 Q. So the answer is no; is that right, sir?</p> <p>2 A. I'm going to make my best effort to answer you</p> <p>3 as responsively as I can.</p> <p>4 I didn't see any evidence about SolarWinds</p> <p>5 being aware of deficiency in the area of network</p> <p>6 monitoring. I didn't see any convincing evidence, any</p> <p>7 that was sufficient for me to form an opinion based on</p> <p>8 SolarWinds' network monitoring practices. I certainly</p> <p>9 saw some evidence that there were, you know, firewalls</p> <p>10 in place all or most of the time that they issued</p> <p>11 reports. That's not sufficient for me to evaluate the</p> <p>12 network monitoring practices.</p> <p>13 Q. So the answer, sir, is no, you did not see any</p> <p>14 documented -- I'll read it again:</p> <p>15 "SolarWinds documented numerous issues</p> <p>16 with network monitoring over the years."</p> <p>17 You didn't see any evidence of SolarWinds</p> <p>18 documenting numerous issues with network monitoring over</p> <p>19 the years, did you?</p> <p>20 A. That's not my evidence -- my testimony is that</p> <p>21 I found insufficient evidence.</p> <p>22 Q. That they were aware of?</p> <p>23 A. It said -- I said -- my twin conclusions were</p> <p>24 that I found insufficient evidence to evaluate the</p> <p>25 practices, and I found insufficient evidence to evaluate</p> <p>149</p>	<p>1 you remember that?</p> <p>2 A. Yes.</p> <p>3 Q. And the SARF forms were designed to provision</p> <p>4 users with access based on their role when they arrived</p> <p>5 at the company. Is that your understanding?</p> <p>6 A. It was part of the processes of -- sure, of</p> <p>7 provisioning, you bet.</p> <p>8 Q. Right. But the purpose was to assign users</p> <p>9 access based on their role. That's what the SARFs were</p> <p>10 for?</p> <p>11 A. Well that was part with the -- and they had a</p> <p>12 section about what were their roles and what you get</p> <p>13 access to and so forth.</p> <p>14 Q. Right. If I was starting as a, whatever, IT</p> <p>15 support person, there would be a set of accesses that I</p> <p>16 would get based on that role, if the SARF process was</p> <p>17 followed?</p> <p>18 A. That's right.</p> <p>19 Q. It sounds like you're not contesting that was</p> <p>20 done at the company as a routine practice?</p> <p>21 A. Yeah, I think that's right.</p> <p>22 Q. And then when people left the company, sort of,</p> <p>23 it would be followed in reverse, right? There would be</p> <p>24 a help desk ticket that would be generated that would</p> <p>25 instruct that the person's access be removed and the IT</p> <p>151</p>
<p>1 whether they were aware of any deficiencies.</p> <p>2 Q. Whether they were aware of any deficiencies, if</p> <p>3 they had documented numerous issues with network</p> <p>4 monitoring over the years, wouldn't there be evidence</p> <p>5 that they were aware of deficiencies in --</p> <p>6 A. Quite likely.</p> <p>7 Q. Okay. Did you see any evidence like that, yes</p> <p>8 or no? If you say yes, I'm going to ask you to point me</p> <p>9 to it. So did you see any?</p> <p>10 A. I'm sorry. Did I see any evidence that they</p> <p>11 were aware of deficiencies in this area?</p> <p>12 Q. Yes.</p> <p>13 A. Not that I recall.</p> <p>14 MR. BRUCKMANN: Serrin, we've been going</p> <p>15 for over an hour. Is this a good time for a</p> <p>16 break?</p> <p>17 MR. TURNER: That's fine.</p> <p>18 THE VIDEOGRAPHER: The time right now</p> <p>19 is 2:15 p.m. and we're off the record.</p> <p>20 (Whereupon, a short break was taken.)</p> <p>21 THE VIDEOGRAPHER: Stand by, please.</p> <p>22 The time right now is 2:34 p.m., and we're back</p> <p>23 on the record.</p> <p>24 Q. Okay. Mr. Graff, I want to talk next about</p> <p>25 access controls. We've talked about the SARF forms. Do</p> <p>150</p>	<p>1 help desk would implement that removal of access.</p> <p>2 Is that your understanding?</p> <p>3 A. That's the way it was supposed to work, and I</p> <p>4 know it did work that way in a lot of cases.</p> <p>5 Q. Right. So with that too, you're not contesting</p> <p>6 that that was the routine practice of the company?</p> <p>7 A. No, I'm not contesting that.</p> <p>8 Q. And how about, did you read about the admin</p> <p>9 access alerts that Mr. Cline and Mr. Quitugua testified</p> <p>10 about? I'm talking about the e-mail alerts that the</p> <p>11 InfoSec team would get when somebody would be added to</p> <p>12 an admin group.</p> <p>13 Do you remember that testimony?</p> <p>14 A. I don't remember that. I would have to see</p> <p>15 that.</p> <p>16 Q. Take a look at Dr. Rattray's report, paragraph</p> <p>17 47.</p> <p>18 A. 47. I see it.</p> <p>19 Q. Just take a look and read that paragraph, if</p> <p>20 you will, most importantly, Mr. Cline's testimony and</p> <p>21 the testimony cited in the footnote.</p> <p>22 A. You're asking me to read it to myself?</p> <p>23 Q. Yes, please.</p> <p>24 A. Okay. You bet.</p> <p>25 Okay. I've read that.</p> <p>152</p>

<p>1 Q. So are you -- are you contesting that these 2 alerts were sent -- let me put it differently. 3 So is it your understanding, based on the 4 testimony you just reviewed, that SolarWinds had a SEM, 5 security event manager, that would automatically detect 6 whether a person was being added to an admin group? 7 A. It does talk about the SEM. Yes, I think -- 8 I'm not sure quite how it worked, but they certainly 9 seemed to have a SEM that received alerts on this case. 10 Q. And when someone was added to an administrator 11 group, the InfoSec team would be alerted? 12 A. That's how Mr. Cline described it, you bet. 13 Q. And the InfoSec team would check to see if the 14 grain of access was authorized and intentional? 15 A. I don't know that part, but that's the 16 procedure he's talking about, yes. 17 Q. And you're not contesting that that was done as 18 a routine practice at the company? 19 A. As a routine practice, no. 20 Q. And do you recall reviewing testimony and 21 evidence about the user access reviews that SolarWinds 22 performed? 23 A. I saw some of that. 24 Q. And these were reviews to make sure that 25 employees' user access rights were appropriately</p> <p>153</p>	<p>1 A. I don't think I have any -- I have no 2 recollection of anything that would contest that. 3 Q. And you're aware that SolarWinds' systems for 4 provisioning access were repeatedly audited during the 5 relevant period? 6 A. They were required to be audited in some ways 7 according to some standards. 8 Q. In particular, there were SOC's audits done in 9 2019 and 2020? 10 A. Yes, I think there were. 11 Q. And those were done by PwC, right? 12 A. That sounds right. 13 Q. And PwC is a reputable auditor in the field, 14 right? 15 A. Yes. 16 Q. And PwC specifically looked at how user access 17 was provisioned on the active directory? Are you aware 18 of that? 19 A. That, I don't recall. I wouldn't be surprised. 20 Q. Can you give me a moment, sir. 21 Okay. So did you work on audits, by the way, 22 when you were at NASDAQ? 23 MR. CARNEY: Objection. Vague. 24 Q. Did you participate in audits in any way? 25 MR. CARNEY: Objection. Vague.</p> <p>155</p>
<p>1 assigned, right? 2 A. That would be the purpose of those, uh-huh. 3 Q. And you're not contesting that those user 4 access reviews were prepared as a regular practice at 5 the company? 6 A. I don't know that I have any information about 7 how regularly it was done, but I know it was a process 8 that they laid out. 9 Q. Have you seen more than 50 user access reviews 10 that have been produced in the litigation? 11 A. I've seen several of them. 12 Q. Have you seen the more than 50 that were -- 13 A. I don't recall what the numbers. 14 Q. Have you reviewed testimony talking about how 15 these were done on a quarterly basis? 16 A. I think I'd want to see that, but that does 17 sound familiar. 18 Q. Okay. So do you have any basis to contest that 19 SolarWinds regularly conducted user access reviews? 20 MR. CARNEY: Objection. Asked and 21 answered. 22 A. I don't have any reason that I can think of to 23 doubt that they conducted them. I don't know how 24 frequently and I don't know how often. 25 Q. But as a regular practice?</p> <p>154</p>	<p>1 A. Well, I was often audited. 2 Q. And how would those audits work at a basic 3 level? The auditors would interview the people who were 4 subject matter experts in the controls they were looking 5 at and then they looked for sample evidence to see that 6 the controls were in place? 7 Is that generally how the process works? 8 A. Yes, and with a particular emphasis not only on 9 what we say, but also the policies we produce and, 10 furthermore, the evidence that we could bring to bare 11 that showed that the policies were being executed. 12 Q. Right. They wouldn't search company e-mails 13 typically, right? 14 MR. CARNEY: Objection. Form. 15 A. Well, I'm not sure. I think perhaps they did 16 in some cases, but I'm not sure. 17 Q. So the audits that were done by PwC didn't find 18 any material weaknesses in the company's system for 19 provisioning access, did they? 20 A. I don't know that I've actually seen the 21 reports from the PwC audit. I do remember some 22 SolarWinds employees talking about SOC's faults, but as 23 to whether that actually showed up in the PwC report, I 24 don't think I have the information on that. 25 Q. Did you not ask for those materials to review</p> <p>156</p>

<p>1 before you put your report together?</p> <p>2 A. I didn't ask -- I don't recall asking for the</p> <p>3 audit reports. Actually, at some point, I think I may</p> <p>4 have asked for the audit reports, but I'm not sure.</p> <p>5 Q. So did you look at them or not?</p> <p>6 A. I don't recall seeing the audit reports. If</p> <p>7 you show me one, I might be able to recognize it, but I</p> <p>8 don't recall seeing it.</p> <p>9 Q. Well, wouldn't that be an important source of</p> <p>10 information to look at? If you had a reputable auditor</p> <p>11 in the field come and audit some of the very controls</p> <p>12 that are at issue in the case, wouldn't you have wanted</p> <p>13 to see what the audit results were?</p> <p>14 A. Well, that kind of goes with the answer I gave</p> <p>15 earlier today that, you know, there are -- I'm sure</p> <p>16 there are many, many documents I didn't look at, and</p> <p>17 some of those probably would have done a good job of</p> <p>18 representing that SolarWinds did what they said they</p> <p>19 did. But my conclusion was that, even if I saw lots and</p> <p>20 lots of additional reports, I would still not change my</p> <p>21 opinion based on the egregious problems that I saw that</p> <p>22 SolarWinds identified.</p> <p>23 Q. Right. So even if an auditor had confirmed</p> <p>24 that role-based access controls were in place and had</p> <p>25 interviewed the employees that were involved, had looked</p> <p style="text-align: center;">157</p>	<p>1 all when you prepared your report?</p> <p>2 MR. CARNEY: Objection. Asked and</p> <p>3 answered. Compound.</p> <p>4 A. I'm not recalling seeing a SOC's audit report.</p> <p>5 I may have. I don't recall. If I could see one, it</p> <p>6 would refresh my memory.</p> <p>7 Q. Okay. But you don't contest that audits were</p> <p>8 done under SOC's and the audits found that role-based</p> <p>9 access controls were in place?</p> <p>10 A. Well, I don't -- I certainly don't contest that</p> <p>11 the audits were done under SOC's as to what the results</p> <p>12 were. As I said, I don't recall having seen any</p> <p>13 reports. I could be mistaken. And there were other</p> <p>14 role-based access problems. I don't know whether they</p> <p>15 got into the reports or not.</p> <p>16 Q. The SEC alleges in its amended complaint that</p> <p>17 SolarWinds "routinely and pervasively granted employees</p> <p>18 unnecessary admin rights."</p> <p>19 Have you seen evidence of that is true, that it</p> <p>20 routinely and pervasively granted employees unnecessary</p> <p>21 admin rights?</p> <p>22 A. Well, I've seen evidence that --</p> <p>23 Q. I don't want to hear about the egregious</p> <p>24 examples of specific issues. I'm talking about</p> <p>25 frequency here. You said you're not making any claim</p> <p style="text-align: center;">159</p>
<p>1 at sample evidence of the controls in place, that</p> <p>2 wouldn't matter because you had seen these egregious</p> <p>3 violations, in your view?</p> <p>4 MR. CARNEY: Objection.</p> <p>5 Mischaracterizes testimony.</p> <p>6 A. I don't know -- like I said, I don't recall</p> <p>7 having seen the audit reports. There were several</p> <p>8 violations that probably would have been shown up in</p> <p>9 SOC's violation reports. I don't know whether the</p> <p>10 auditors found them or not.</p> <p>11 Q. So it's your contention that -- I just want to</p> <p>12 go back, though. Basically -- it sounds like your</p> <p>13 position is after seeing these -- as you put it --</p> <p>14 "egregious issues" that you identified in your report,</p> <p>15 it wouldn't matter what other documents you saw because</p> <p>16 those egregious issues by themselves implied to you that</p> <p>17 SolarWinds' statements in their security statement were</p> <p>18 not true?</p> <p>19 A. Well, I stated precisely in my report, but</p> <p>20 that's the gist of it, that I saw enough in the examples</p> <p>21 I cited to make a decision, to form an opinion.</p> <p>22 Q. Okay. So is it -- I just want to be clear.</p> <p>23 Did you consider the auditors' conclusions and disregard</p> <p>24 them because you thought the egregious issues you saw</p> <p>25 were more important or did you just not consider them at</p> <p style="text-align: center;">158</p>	<p>1 about frequency, and so I'm asking you whether you've</p> <p>2 seen any evidence that SolarWinds routinely and</p> <p>3 pervasively granted employees unnecessary admin rights?</p> <p>4 A. I don't know -- I don't know that I would</p> <p>5 characterize it as a routine failure. I certainly saw</p> <p>6 several examples of failures in processes. But there's</p> <p>7 a problem with the word "routinely" too, because there</p> <p>8 were issues that lasted months and years, so do you</p> <p>9 count that as one instance or more than one?</p> <p>10 Q. So here we're talking about, not particular</p> <p>11 issues, we're talking about employees being granted</p> <p>12 admin rights.</p> <p>13 Did you see evidence that employees pervasively</p> <p>14 at the company were granted admin rights?</p> <p>15 A. I saw evidence of some employees being given</p> <p>16 superuser access rights that weren't related to their</p> <p>17 roles, and it happened more than once, but whether that</p> <p>18 would match the characterization of frequently or</p> <p>19 routinely, I don't think so.</p> <p>20 Q. Let's take a look at that issue, the billing</p> <p>21 system user, or the superuser access issue that you just</p> <p>22 mentioned.</p> <p>23 (Whereupon, SW-SEC-SDNY_00254254-266</p> <p>24 was marked as Graff Exhibit 11, for</p> <p>25 identification, as of this date.)</p> <p style="text-align: center;">160</p>

Mark Graff
2/14/2025

<p>1 Q. Do you recognize this e-mail chain, Mr. Graff?</p> <p>2 A. It's got several pages to it. Just let me just</p> <p>3 take a quick look.</p> <p>4 Q. Sure.</p> <p>5 A. Yes, I've seen this before.</p> <p>6 Q. And this is that superuser issue you were just</p> <p>7 mentioning, right?</p> <p>8 A. I think there may have been more than one, but</p> <p>9 this is certainly a superuser issue.</p> <p>10 Q. This issue concerned a group of developers in</p> <p>11 Biz Apps who were working on a project to improve</p> <p>12 SolarWinds' billing system?</p> <p>13 A. Yes. It was the primary issue that was raised</p> <p>14 initially.</p> <p>15 Q. And those developers needed access to billing</p> <p>16 data in production to test the system they were working</p> <p>17 on.</p> <p>18 Is that your understanding?</p> <p>19 A. Well, I don't know they needed it. The</p> <p>20 developers thought they needed it, and they were given</p> <p>21 it for that reason, the core practice.</p> <p>22 Q. So the developers thought they needed access to</p> <p>23 the data --</p> <p>24 A. I think we know that -- I'm sorry, please</p> <p>25 finish your question.</p> <p>161</p>	<p>1 current situation was -- the solution that they came up</p> <p>2 with was that Biz Apps would be granted superuser access</p> <p>3 to the new API, which would unblock us, and we could</p> <p>4 move forward with our backup for 365 billing project,</p> <p>5 and the long-term solution was create a read-only role</p> <p>6 that Biz Apps would use access production data for</p> <p>7 backup billing and for backup of 365 billing.</p> <p>8 So in other words, they were granted superuser</p> <p>9 access at the time, that was the solution proposed,</p> <p>10 because there was no read-only role that was available</p> <p>11 at the time of this e-mail?</p> <p>12 A. That's the way they saw it.</p> <p>13 Q. And your contention is that this is an</p> <p>14 egregious -- egregious what? Violation of --</p> <p>15 A. I said in my report, actually, this arrangement</p> <p>16 violates several principles.</p> <p>17 Q. And I don't want to -- right now, I just want</p> <p>18 to focus on role-based access controls. I'm not</p> <p>19 concerned about separation of the production from the</p> <p>20 development environment.</p> <p>21 So if we could just talk about how this</p> <p>22 document implies that anything the security statement</p> <p>23 says about role-based access controls was false?</p> <p>24 A. I'd want to look at my report briefly to look</p> <p>25 at this discussion. And I found it. Let's see. I'll</p> <p>163</p>
<p>1 Q. The developers thought they needed it, right?</p> <p>2 A. Either the developers or their manager.</p> <p>3 Q. And at the time, the only way to give them</p> <p>4 access to the data was to give them superuser access to</p> <p>5 the relevant API because there wasn't a read-only access</p> <p>6 available?</p> <p>7 A. I don't think -- I can't agree that was the</p> <p>8 only way to do it. There are other methods they might</p> <p>9 have considered.</p> <p>10 Q. Did you see anything in this e-mail chain that</p> <p>11 indicate otherwise? Wasn't that the issue, is that the</p> <p>12 -- there was no read-only access available with respect</p> <p>13 to the API at issue, so the proposal was to give them</p> <p>14 superuser access so that they can utilize the data,</p> <p>15 access the data? If you want to take a look at page 2</p> <p>16 of the document, the one Bates ending in 255.</p> <p>17 I'll just note for the record that the Bates</p> <p>18 stamp of this document is SWSEC00254254.</p> <p>19 A. So could I have the question again, please.</p> <p>20 Q. Do you want to familiarize yourself with the</p> <p>21 page or --</p> <p>22 A. I'm on page 3. It was on page 2?</p> <p>23 Q. On page 2, please.</p> <p>24 A. Yes, I see it.</p> <p>25 Q. Okay. So after this whole e-mail chain, the</p> <p>162</p>	<p>1 be quick. I'm looking for the section on the superuser</p> <p>2 access, if anybody has a page number that would speed</p> <p>3 this up.</p> <p>4 Q. I think it's on page 37.</p> <p>5 A. That was one area.</p> <p>6 Q. It comes up in a few places?</p> <p>7 A. It does come up in a few places.</p> <p>8 Q. So maybe we'll jump up to paragraph 155.</p> <p>9 MR. CARNEY: Paragraph 79 would be</p> <p>10 another one.</p> <p>11 THE WITNESS: I'm going to put a finger</p> <p>12 in 79 and 155. I'm sure one of those is right.</p> <p>13 Let's see.</p> <p>14 Q. Okay. Yeah, that's fine. I'll focus on</p> <p>15 paragraph 84.</p> <p>16 A. Okay. All right.</p> <p>17 Q. Because you say:</p> <p>18 "The existence of this incident is</p> <p>19 indicative of a deeper issue than a one-off</p> <p>20 error."</p> <p>21 First of all, I want to understand what the</p> <p>22 error is. As you said, the developers wanted the access</p> <p>23 in order to work on a billing project, right?</p> <p>24 A. That's my understanding.</p> <p>25 Q. So they thought they needed the access, and</p> <p>164</p>

Mark Graff
2/14/2025

<p>1 And then if you see, on the left-hand side, Biz 2 Apps billing BV is the issue? 3 MR. CARNEY: Yeah. 4 Q. Okay. So is it your contention, Mr. Graff, 5 because you say in that paragraph earlier, that we look 6 at in paragraph 84, the existence of this incident was 7 indicative of a deeper issue than a one-off error, are 8 you -- are you contending that this -- this incident 9 reflects some sort of pervasive failure to implement 10 role-based access controls or something different? 11 A. This incident is indicative of several -- yes, 12 it's several pervasive issues among others having to do 13 with role-based access control. 14 Q. Okay. So are you -- are you asserting that 15 this incident shows that role-based access controls -- 16 there was a pervasive failure to implement role-based 17 access controls? 18 A. Not necessarily by itself, but to give you 19 one-sentence answer, they're granting write access to 20 developers in production of live data. That's a 21 role-based access control problem that's very serious, 22 and there are other problems too. 23 Q. Sir, I don't want to talk about the issue of 24 dividing production environment from development 25 environment. Okay. I just want to focus on the issue</p> <p>169</p>	<p>1 in your report. So Mr. Brown determined that the 2 developers needed this access, so the developers were 3 getting access based on what they needed to do their 4 job, based on Mr. Brown's understanding, correct? 5 A. Actually, he determined they needed access to 6 the data. They were given read-write access to the 7 data, which is vastly different. He can accept the risk 8 on that, but their need to have write access to the data 9 is not clear. 10 Q. There was no read-only option at the time, so 11 in order to avoid delaying a major project, they needed 12 read and write access in order to complete their 13 project; isn't that right? 14 A. A corporation, in fact, can determine that they 15 want to compromise that principle and accept the risk. 16 Q. Compromise what principle? The principle is 17 employees getting access based on what they need to do 18 for their role. Here there was a determination made 19 that, in order to perform their role, they needed this 20 access at the time. The company was entitled to make 21 that determination, was it not? 22 A. Yes. 23 Q. Now, in terms of the pervasiveness of this 24 issue, whatever you want to call it, this only related 25 to a single customer billing system, that's all we're</p> <p>171</p>
<p>1 of whether SolarWinds implemented role-based access 2 controls. 3 And in terms of how pervasive this issue was, 4 let's just start out as to whether it was an access 5 issue at all. They needed this access -- the developers 6 needed this access in order to complete the project. 7 That was Mr. Brown's finding, right? 8 A. I don't know that he found it that way. He 9 said it -- he approved the risk assessment form. And he 10 evaluated it as a low risk. I think the risk was 11 misrepresented in this spreadsheet. 12 Q. In Column D, under Benefits of Accepting This 13 Risk, Mr. Brown wrote: 14 "It allows Biz Apps dev to continue the 15 development work and not delay a major 16 projects." 17 And Mr. Brown, who was head of the InfoSec 18 team, determined that the developers needed this access 19 to continue the development work and not delay a major 20 project. Isn't that a correct statement of the facts? 21 A. Somebody concluded that they needed that access 22 to continue the development work. I read the e-mail 23 chain. 24 Q. I'll ask you to assume it was Mr. Brown who 25 made that determination. I believe that's what you say</p> <p>170</p>	<p>1 talking about here, right? Superuser access to certain 2 APIs connected to a billing system? 3 A. When I talk about a pervasive issue, I'm also 4 discussing the design problem that created this issue. 5 Q. The design problem -- you're talking about the 6 lack of a read-only permission? 7 A. Well, there are many design problems. But that 8 was one of them. 9 Q. Okay. That is a design specific to this 10 billing system that we're talking about, right? There's 11 no other system that is mentioned in any of these 12 communications in the e-mail chain we're looking at, 13 right? 14 A. This is the only one mentioned in that e-mail 15 chain, that's right. 16 Q. Right. So you can't infer from this e-mail 17 that SolarWinds' systems were pervasively designed to 18 give everyone read and write access; you're not drawing 19 that conclusion, are you? 20 A. No. There are other conclusions I'm drawing 21 from it, but not that one. 22 Q. And this chain is just about granting access to 23 a specific team of developers, the Biz App developers, 24 right? 25 A. No. I say it's about a lot more than that.</p> <p>172</p>

Mark Graff
2/14/2025

<p>1 Q. Well I'm talking about in terms of the scope of 2 the issue we're talking about. You're concerned that -- 3 about the grant of access to this API, and here we're 4 just talking about a specific group of developers 5 working on a specific project. Those are the only 6 people that Mr. Brown is authorizing that access for, 7 correct?</p> <p>8 A. There was one specific group of people that 9 needed access, were declared to have needed access, and 10 they were given read-write access using shared log-ins 11 on live production data, so I'm not going to just talk 12 about just role-based access control problems.</p> <p>13 Q. Mr. Graff, just to be clear, Mr. Brown was not 14 authorizing them to share some account, talking about 15 that was what happened before that raised this issue up 16 to security in the first place.</p> <p>17 A. Yes.</p> <p>18 Q. But the solution was to give them each super 19 user credentials so that they could complete this 20 project. So let's keep shared credentials out of it.</p> <p>21 I'm just talking about right now the principle 22 of role-based access, assigning employees the access 23 they need to perform their role. And am I right, that 24 in this case, we're talking about a single group of 25 developers getting access to a single system?</p> <p>173</p>	<p>1 Q. Now, you cite this document repeatedly in your 2 report, correct?</p> <p>3 A. Yes.</p> <p>4 Q. Now, first of all, would you agree, Mr. Graff, 5 this is a draft document, right? There are a number of 6 pages here that are just incomplete or in draft form?</p> <p>7 A. Yeah, could be characterized as a draft report. 8 The reports I was quoting are in black and white.</p> <p>9 Q. Well, they are in black and white, but you 10 don't know whether these are just someone's initial 11 thoughts or final conclusions?</p> <p>12 A. I don't know that.</p> <p>13 Q. You don't know if anyone vetted what's in here 14 or approved what's in here?</p> <p>15 A. No, there are -- well, there are e-mails that 16 talk about it further. So there's other discussions 17 about it, but yes.</p> <p>18 Q. But you don't know whether this particular 19 material was approved by anyone or vetted by anyone?</p> <p>20 A. I don't think I do.</p> <p>21 Q. And no one testified about this deck during 22 deposition testimony in this case, as far as you're 23 aware of, right?</p> <p>24 A. Not that I recall. I know they testified about 25 the problems, but I don't think they testified about</p> <p>175</p>
<p>1 A. Yes, and they needed read access for their 2 jobs, and not read/write access for their jobs.</p> <p>3 Q. But no read access was available as part of the 4 APIs, and so as a practical matter, they needed the 5 read/write access to do the task at hand; that was the 6 determination Mr. Brown made?</p> <p>7 A. The company is within its right to make that 8 exception to the role-based access roles.</p> <p>9 Q. Okay. So this was a -- you're not contending 10 that this shows that SolarWinds just pervasively granted 11 everybody read/write access to all their systems; this 12 was a single exception related to a particular team and 13 a particular system?</p> <p>14 A. This particular incident, yes.</p> <p>15 Q. Okay. Let me also ask you about the MSP 16 customer support access issue that you raised earlier.</p> <p>17 (Whereupon, SW-SEC00631418-427 was 18 marked as Graff Exhibit 14, for identification, 19 as of this date.)</p> <p>20 Q. Sir, I'm showing you what's been marked as 21 Graff Exhibit 14, Bates stamped SW-SEC00631418. It's a 22 deck or a draft deck titled "MSP Support Security 23 Improvement."</p> <p>24 Do you see that?</p> <p>25 A. Yes, I do.</p> <p>174</p>	<p>1 this deck. I could be wrong.</p> <p>2 Q. No one testified about the issues raised in 3 this draft deck, as far as you're aware?</p> <p>4 A. I'd have to think about that a bit. I know 5 I've seen a lot of material about it.</p> <p>6 Q. Well, if I represent to you there's no is 7 testimony about this slide deck, do you have any basis 8 to disagree with me?</p> <p>9 A. No.</p> <p>10 MR. CARNEY: Objection. That's a 11 different question.</p> <p>12 A. That's a different question. So what is the 13 question, so that I can agree to it.</p> <p>14 Q. So let's talk about the substance of what's on 15 page 2. Mr. Graff, this appears to be about the systems 16 that SolarWinds MSP customer support staff could use to 17 assist customers of certain MSP products?</p> <p>18 A. Yes.</p> <p>19 Q. By the way, do you know how much -- do you know 20 whether the MSP side of SolarWinds' business was a large 21 or a relatively small portion of their business?</p> <p>22 A. I don't know.</p> <p>23 Q. And it appears from this deck that support 24 personnel had certain abilities to access customer 25 environments?</p> <p>176</p>

<p>1 A. Right.</p> <p>2 Q. And that's not necessarily unusual in the</p> <p>3 industry, is it, for customer support to have some level</p> <p>4 of access or remote login capability to provide customer</p> <p>5 support?</p> <p>6 A. I agree with that.</p> <p>7 Q. But here, there was some concern that MSP</p> <p>8 customer support personnel had more access than they</p> <p>9 might need to customer environments?</p> <p>10 A. Yes, that was part of the problem.</p> <p>11 Q. And so the person who wrote this deck evidently</p> <p>12 was thinking about ways to reduce that access?</p> <p>13 A. Yes, they were talking about security</p> <p>14 improvements related to it.</p> <p>15 Q. And, again, this was an issue that related to</p> <p>16 specific customer support systems used by specific</p> <p>17 personnel within SolarWinds?</p> <p>18 A. Well, it's certainly referring to a specific</p> <p>19 system, which is the MSP support portal.</p> <p>20 Q. Right. And that's a system that MSP customer</p> <p>21 support would have access to, but you have no reason to</p> <p>22 believe that people at the company had access to it</p> <p>23 generally?</p> <p>24 A. I don't know if I recall any report of</p> <p>25 inappropriate access other than the one described by the</p> <p style="text-align: center;">177</p>	<p>1 A. Let's see where that would be. I'm looking for</p> <p>2 the section on MSP as it relates to access control.</p> <p>3 MR. CARNEY: Maybe page 33. Paragraph</p> <p>4 67.</p> <p>5 THE WITNESS: Yes, that's the right</p> <p>6 reference. Thank you.</p> <p>7 Please continue.</p> <p>8 Q. And just to be clear, this document is not</p> <p>9 about limiting employee access to SolarWinds'</p> <p>10 environment, it's about limiting access to SolarWinds</p> <p>11 customers' environments?</p> <p>12 A. Yes, that's right. That's what the expressed</p> <p>13 concern was about.</p> <p>14 Q. And these customers -- the SolarWinds'</p> <p>15 customers are obviously corporations, right, companies?</p> <p>16 A. Yes, that would be right.</p> <p>17 Q. And if a company had a concern about</p> <p>18 SolarWinds' personnel being able to access their</p> <p>19 environment, they could raise that with SolarWinds,</p> <p>20 right?</p> <p>21 A. Sure, especially if they knew what kind of</p> <p>22 access that SolarWinds had.</p> <p>23 Q. And it's not uncommon for companies to build in</p> <p>24 contractual limitations about the sort of access that a</p> <p>25 vendor might have to their environment?</p> <p style="text-align: center;">179</p>
<p>1 other -- referenced to the support team.</p> <p>2 Q. Yeah, and it talks in here about a support</p> <p>3 person having, you know, too much access. So we're</p> <p>4 talking about customer support personnel would be the</p> <p>5 ones using this system?</p> <p>6 A. That's the report, and again, I have to point</p> <p>7 out, that's if everything works the way it's supposed</p> <p>8 to. That's the way it would work.</p> <p>9 Q. Yeah, and you have no reason to believe that</p> <p>10 things didn't work the way they were supposed to? You</p> <p>11 have no reason to believe that anybody other than</p> <p>12 customer support personnel had access to this system?</p> <p>13 A. That's right. I have no reason to believe that</p> <p>14 others did have access to this portal, that I can</p> <p>15 remember, at least. I'll look later in my report about</p> <p>16 this.</p> <p>17 Q. So, again, I just want to be clear on what</p> <p>18 we're talking about. You're not arguing from this</p> <p>19 document that SolarWinds' employees generally had</p> <p>20 excessive access; you just pointed to this as an</p> <p>21 instance where a particular set of employees had more</p> <p>22 access than they needed within a particular system?</p> <p>23 A. I think that's right. I would like to just</p> <p>24 refer to my report briefly.</p> <p>25 Q. Sure.</p> <p style="text-align: center;">178</p>	<p>1 A. That's right.</p> <p>2 Q. So they could do that, too?</p> <p>3 A. Yes.</p> <p>4 Q. Now, this is another issue you characterize as</p> <p>5 "major," right?</p> <p>6 A. Well, I have to look, but I think it probably</p> <p>7 is.</p> <p>8 Q. In fact, you call it "potentially</p> <p>9 catastrophic"?</p> <p>10 A. It's excessive, and I'd have to take your word</p> <p>11 for it as potentially catastrophic, but that does sound</p> <p>12 familiar. Do you have that reference?</p> <p>13 Q. Paragraph 73?</p> <p>14 A. That's right.</p> <p>15 Q. And that's because of the risk of an insider --</p> <p>16 an insider threat?</p> <p>17 A. Yes, if we include in the idea of an insider</p> <p>18 threat the idea of an attacker taking control of this,</p> <p>19 so he becomes an insider. He becomes -- he poses as a</p> <p>20 cybersecurity employee with valid access and then moves</p> <p>21 onto the customer data. That's what I -- one of the</p> <p>22 things I was talking about.</p> <p>23 Q. Right. So the attacker would have to get into</p> <p>24 SolarWinds somehow, hack into a customer support staff's</p> <p>25 account, learn how to use the software, and then use it</p> <p style="text-align: center;">180</p>

<p>1 to compromise customers?</p> <p>2 A. There are other ways, but that's probably the</p> <p>3 primary way.</p> <p>4 Q. Are you aware of either scenario ever happening</p> <p>5 at SolarWinds up to the point of time in this slide?</p> <p>6 A. I know there was a discussion of the incidents</p> <p>7 that already had occurred as a result of inappropriate</p> <p>8 access. I don't know what the details of the access</p> <p>9 were.</p> <p>10 Q. Well, they weren't malicious, right? There was</p> <p>11 some accidental access but --</p> <p>12 A. I'd have to look that up. I'm not sure I have</p> <p>13 the details on the incidents.</p> <p>14 Q. Can you point to any malicious incident that</p> <p>15 you're aware of sitting here today that occurred due to</p> <p>16 this issue, before this slide?</p> <p>17 A. No.</p> <p>18 Q. So this was a risk, right?</p> <p>19 A. There was some incidents, but yes, I was mostly</p> <p>20 focusing on the risk by -- entailed in this arrangement.</p> <p>21 Q. And just having a risk doesn't mean the risk is</p> <p>22 likely to materialize? It hadn't materialized by this</p> <p>23 point?</p> <p>24 A. It's not -- it doesn't mean it's likely to</p> <p>25 materialize. I have no information about whether it</p> <p style="text-align: center;">181</p>	<p>1 and inadvertently created 400-plus tickets in a</p> <p>2 customer's PSA."</p> <p>3 I can represent to you that a PSA was part of</p> <p>4 the product involved. So that was obviously an</p> <p>5 accident. That accident brings this risk to the</p> <p>6 company's attention, and they're trying to mitigate the</p> <p>7 risk before there's some sort of insider threat incident</p> <p>8 like you'd mentioned previously. Is that a fair</p> <p>9 assessment of what's going on here?</p> <p>10 A. That surely -- yes, that characterizes the</p> <p>11 second bullet correctly. I think the first bullet,</p> <p>12 which talks about how they were diagnosing a user remote</p> <p>13 session and so forth, so I'm not sure that would be</p> <p>14 accidental because it triggered the defensive, you know,</p> <p>15 notification on the client's side. But it doesn't</p> <p>16 certainly indicate any kind of maliciousness.</p> <p>17 Q. Okay. That's all I'm getting at.</p> <p>18 Now, just generally though, isn't this what a</p> <p>19 good cybersecurity program is supposed to do, when risks</p> <p>20 arise, take steps to mitigate them?</p> <p>21 A. Right.</p> <p>22 Q. And, again, the security statement doesn't say</p> <p>23 anywhere that SolarWinds' access controls were perfect?</p> <p>24 A. That's true.</p> <p>25 Q. And did you ever hear the term "continuous</p> <p style="text-align: center;">183</p>
<p>1 eventuated or not.</p> <p>2 Q. But SolarWinds here was proactively taking</p> <p>3 action to mitigate this risk before something happened?</p> <p>4 A. Well, I'm not sure I would say it was proactive</p> <p>5 since there was an internal report about the problem,</p> <p>6 and then there -- so that's -- that's after the fact,</p> <p>7 when it was instituted, and then they were also talking</p> <p>8 about the fact that incidents had already taken, so I'm</p> <p>9 not sure that's proactive either.</p> <p>10 Q. Let's be clear, Mr. Graff.</p> <p>11 A. Mm-hmm.</p> <p>12 Q. The incident that already happened was -- if</p> <p>13 any incidents had happened before this, they were</p> <p>14 accidental, not malicious, so there had been -- that had</p> <p>15 led to the observation of this issue, and now there was</p> <p>16 an effort to fix it before there was some sort of</p> <p>17 malicious exploitation of the risk?</p> <p>18 MR. CARNEY: Objection. Compound.</p> <p>19 Q. You understand the question?</p> <p>20 A. No. I'd like to hear the question.</p> <p>21 Q. Okay. So if you look -- and apologies if this</p> <p>22 is so hard to read. I had hoped we'd get better</p> <p>23 slides -- but if you look on the slide it indicates:</p> <p>24 "While testing release, the SolarWinds</p> <p>25 engineering team copied a customer environment</p> <p style="text-align: center;">182</p>	<p>1 improvement"?</p> <p>2 A. Yes, I have heard that term.</p> <p>3 Q. And people in the industry generally understand</p> <p>4 that cybersecurity is a process of continuous</p> <p>5 improvement; wouldn't you say that's a commonly -- a</p> <p>6 common notion in the industry?</p> <p>7 A. Yes.</p> <p>8 Q. And a company engaged in continuous improvement</p> <p>9 will identify risks from time to time that need to be</p> <p>10 addressed; that's what it involves, continue</p> <p>11 improvement?</p> <p>12 A. Well, sometimes they identify it. Sometimes,</p> <p>13 as in these cases, a customer alerts them, or an</p> <p>14 independent security researcher alerts them, and that</p> <p>15 happened in these cases, but yes, that's part of the</p> <p>16 process, is to find out about problems and then go fix</p> <p>17 them and improve things.</p> <p>18 Q. And that process doesn't imply that you don't</p> <p>19 have controls to begin with?</p> <p>20 A. Well, some of the incidents would, but the</p> <p>21 process of finding out about it and fixing it by itself</p> <p>22 doesn't indicate that you don't have controls.</p> <p>23 Q. And going back to the NASDAQ incident, right,</p> <p>24 so a major incident like that happens, it doesn't mean</p> <p>25 that the company didn't have business continuity</p> <p style="text-align: center;">184</p>

<p>1 controls but it means there's an issue that needs to be 2 fixed.</p> <p>3 A. Yeah, there were flaws in the software and I 4 think in the business continuity controls at NASDAQ at 5 that time, absolutely.</p> <p>6 Q. And so here, you see SolarWinds kind of doing 7 the same thing. It wasn't an incident that happened, 8 but it was a risk that had been observed, and the 9 company is taking action to mitigate that risk?</p> <p>10 A. Well, they classified that as an incident.</p> <p>11 Q. Where do you see that?</p> <p>12 A. I'm not sure I have that exact record, but I 13 will say that in my study of the policies relating to 14 their incident management, they did find -- they did 15 classify software issues that arose as incidents, and 16 that's what I was referring to.</p> <p>17 MR. CARNEY: If I could just direct you 18 to the slide you were showing him, it uses the 19 word "incident."</p> <p>20 THE WITNESS: Yeah, it does.</p> <p>21 Q. You're talking about the accidental -- the -- 22 whatever, the ones under the second heading there?</p> <p>23 A. Yeah, the two bullets that talked about the 24 things that happened, yes, those are -- those are 25 referred to as incidents, and that was the way that</p> <p style="text-align: center;">185</p>	<p>1 employee. Do you know what I'm referring to?</p> <p>2 A. I do remember that, yes.</p> <p>3 Q. I just first want to get clear, this is on page 4 54 of your report?</p> <p>5 A. Thank you. Yes, I have it. It's paragraph 98, 6 I think.</p> <p>7 Q. And so you say, this SARF document shows an ad 8 hoc process, and then you continue:</p> <p>9 "As shown below, SolarWinds employees 10 discussed that because they do not know the 11 termination date of a temp, i.e., a temporary 12 worker, they decide to provide his account with 13 a one-year expiration date." 14 And then you quote a chat where they're 15 discussing what end date to put for the employee.</p> <p>16 MR. CARNEY: Object to the 17 characterization.</p> <p>18 Q. Is that a fair characterization?</p> <p>19 MR. CARNEY: The word "chat."</p> <p>20 MR. TURNER: I believe it's a chat, but 21 if you want to tell me it's something else, go 22 ahead.</p> <p>23 A. I remember the SARF in question, I remember 24 what I said about it, and just to be clear, when you 25 quoted there, in paragraph 98, it said, "This issue is</p> <p style="text-align: center;">187</p>
<p>1 SolarWinds characterized, quite often, software issues.</p> <p>2 Q. Right. Right. But these weren't -- like you 3 said before, these weren't malicious incidents; these 4 were just incidents where something wrong had happened 5 that basically flagged a risk?</p> <p>6 A. Well, I see no evidence that it was malicious.</p> <p>7 Q. Right. But you'd agree here -- what you see 8 here is consistent with the concept of continue 9 improvement?</p> <p>10 A. Well, the fact that they've identified a 11 problem and they're going to try to address it, that's 12 part of it. The fact that the thing happened to begin 13 with and it existed, that's not an example of 14 improvement.</p> <p>15 Q. There's all sorts of risks that can be 16 identified from time to time; that's what happens in the 17 cybersecurity program, right?</p> <p>18 A. Sure, and there are incidents like this one 19 that happen that will trigger analysis and improvements.</p> <p>20 Q. Let me ask you about a different issue. And 21 maybe you could tell me you don't really place much 22 weight on this issue. But you mention in your report a 23 single SARF that you say shows an ad hoc process because 24 employees provided an account with a one-year expiration 25 date when they didn't know the termination date for the</p> <p style="text-align: center;">186</p>	<p>1 illustrated in a SARF document," and the issue I'm 2 talking about is described in paragraph 97 where 3 Ms. Ronnie Johnson talked about that SolarWinds and 18 4 individuals did access the systems after they left 5 SolarWinds, and there were other incidents we can talk 6 about that relate to that, too. So that's what this is 7 an illustration of.</p> <p>8 Q. Well, I'm unclear how this is an illustration 9 of that. Are you saying that what's described in 10 paragraph 98 shows that somebody's access was not 11 terminated in a timely fashion after they left the 12 company?</p> <p>13 A. What's illustrated in that form that I cited is 14 that there was a very casual -- in that instance, there 15 was a very casual ascertainment of how long access 16 should be retained. And they said -- they'd make it -- 17 I forget the exact wording, but it was something along 18 the lines of, well, we think it will be about a year, 19 something like that, and then we can terminate it later.</p> <p>20 So I thought that was an indication of perhaps 21 poor training or an ad hoc process. But I felt it was 22 related to the other issues that I identified about lack 23 of termination.</p> <p>24 (Whereupon, SW-SEC-SDNY_00050922 was 25 marked as Graff Exhibit 15, for identification,</p> <p style="text-align: center;">188</p>

Mark Graff
2/14/2025

<p>1 Q. But, sir, you cited this as an example, when, 2 in fact, the person may not have needed an end date 3 because they were being hired to work at SolarWinds for 4 much longer than that? 5 A. Good practice would have indicated that they 6 would give some idea of how long they were going to be 7 there. If they knew they were going to be indefinitely, 8 then they should say that when they request. That's the 9 norm. When you request access for someone, you give an 10 idea of how long they are going to be there. If you 11 think it's a very long assignment, you can say that. 12 You can have it for one period, a year, something 13 longer, but you should be specifying how long that 14 access is for and what they should have access to. 15 Q. SolarWinds had a practice, I think we mentioned 16 earlier, of sending a separate ticket when a person was 17 actually terminated, right? We talked about that 18 earlier. 19 Do you remember that? 20 A. I do remember that. 21 Q. And I think you said earlier you don't have any 22 reason to believe that didn't occur as a regular 23 practice. Now, all the security statement says about 24 termination is it says: 25 "Processes and procedures are in place</p> <p>193</p>	<p>1 least privilege not followed as a best practice." 2 Do you see that? 3 A. Yes. 4 Q. Now, without more context, do you have any way 5 of knowing exactly what this notation refers to? 6 A. Well, I understand what least privilege is. 7 And I understand several -- more than one example of 8 when the least privilege wasn't followed. I don't know 9 precisely what examples they're talking about in this. 10 Q. Yeah, I'm not asking you to define for me the 11 principle of least privilege. I'm asking you to -- 12 whether you understand the specific problem here related 13 to least privilege that this might relate to? 14 A. I don't recall seeing any details that would 15 explain precisely what the problem is that -- what 16 incident or issue led to that notation. 17 Q. Right. So this is a sort of document, right, 18 where you need more context provided, for example, by 19 the person who prepared this slide to understand what 20 was meant today? 21 A. You certainly can't understand precisely what 22 he was talking about. And, now, I haven't studied the 23 entire document lately, so it may have more information 24 in there, but on that basis, I certainly can't tell 25 exactly what he might have been referring to.</p> <p>195</p>
<p>1 to address employees who are voluntarily or 2 involuntarily terminated." 3 Would you agree that having a process or 4 procedure where tickets are sent to the help desk when 5 somebody is terminated to terminate their access, 6 there's a process and procedure to address employees who 7 are terminated? 8 A. Yes. 9 Q. So aside from these three -- strike that. 10 Let's look at a few other documents you cite 11 in relation to access controls. 12 You doing okay, Mr. Graff, or do you need a -- 13 A. I'm good, thank you. 14 (Whereupon, SW-SEC00012266-275 was 15 marked as Graff Exhibit 17, for identification, 16 as of this date.) 17 Q. So I'm showing you what's been marked as Graff 18 Exhibit 17, and it's a slide deck titled "Major Project 19 Portfolio," bearing the date January 2018 with a Bates 20 stamp SW-SEC12266. 21 Do you see that? 22 A. I see it. 23 Q. And you cite the third page of this document. 24 And, particularly, you cite the notation on the 25 left-hand side of the slide that says: "Concept of</p> <p>194</p>	<p>1 Q. Right. And Mr. Quitugua testified about this, 2 as you may recall, and he specifically testified, and 3 I'm quoting here this notation: "Doesn't indicate that 4 it was a problem across the organization," instead, he 5 testified that: "It may have been found that a 6 particular system wasn't following the concept of least 7 privilege." 8 Do you remember that? 9 A. Yes. 10 Q. So you don't have any basis to conclude that 11 this document relates to a problem across the 12 organization? 13 A. Well, it is talking about enterprise access 14 management standards and audits, so that's what I can 15 tell from it. 16 Q. So what are you saying? That based on that 17 title, you're going to discredit Mr. Quitugua's 18 testimony and conclude that this relates to a problem 19 across the organization? 20 MR. CARNEY: Do you want to direct him 21 to where he said it in the report? 22 Q. Can you answer the question, Mr. Graff? 23 A. I'd need more information about this before I 24 can -- I mean I haven't seen it in a long time, so I 25 need a little help recollecting what this is about and</p> <p>196</p>

Mark Graff
2/14/2025

<p>1 MR. CARNEY: And both the footnotes to 2 the paragraph. 3 THE WITNESS: Right. 4 A. Yeah, I see Footnote 81, and it seems to 5 pertain to the document that you were referring to. 6 Q. So here even in the text, Mr. Graff, you're 7 basically saying Mr. Quitugua said that not all systems 8 were following the concept of least privilege, which is 9 consistent with what we're saying here, that as part of 10 the assessment, it may have been found that a particular 11 system was not following the concept of least privilege. 12 Again, my only question, Mr. Graff, is that you 13 don't have any -- you're not contesting Mr. Quitugua's 14 testimony in any way? 15 A. Well, I'm confused, because in Footnote 81, it 16 says -- he's saying -- the question was -- they're 17 talking about the security statement and the concept of 18 least privilege, and the question is: 19 "So what you're telling me is, at least 20 with respect some systems, that wasn't the 21 case." 22 And he answered, "For a subset of 23 systems that we identified that weren't, you 24 know, for whatever reason, we identified that 25 they weren't following the best practices we</p> <p>201</p>	<p>1 Q. I'm just asking with respect to the meaning of 2 this document? 3 A. Yes, with respect to the meaning of this 4 particular document, that was a statement that seemed to 5 indicate that there was some problem, at least with some 6 system, I don't know exactly which system it is, I'd 7 have to look at the document to be clear, but he 8 identified an issue and he raised it and there were 9 other reasons for that opinion as well. 10 Q. And if you look at the title of the slide, this 11 is about an audit that was being done at the time, 12 right? If you look at the milestones, it talks about 13 the milestones as part of a risk audit and risk 14 assessment? 15 A. Well, I see the title says: "Enterprise Access 16 Management Standards and Audit." 17 Q. And do you see on the right-hand side under Key 18 Milestones/Status? 19 A. "Conduct risk audit and risk assessment against 20 privileged and nonprivileged user accounts, and that's 21 complete as of the end of November 2017." 22 Q. Right. And the whole purpose of an audit, 23 right, is to identify, you know, systems that aren't in 24 compliance? 25 A. Some auditors look at it that way, but</p> <p>203</p>
<p>1 described." 2 So -- so the particular presentation with that 3 slide that I cited, it's only part of a larger picture, 4 because we've got statements from Mr. Quitugua and 5 statements from Mr. Brown both that talk about this. 6 Q. No. This is all Mr. Quitugua -- this is all 7 Mr. Quitugua's testimony. He was the author of this 8 slide. 9 A. That's right. I was talking about what 10 Mr. Brown said about it as well. 11 Q. You don't quote Mr. Brown anywhere. I think -- 12 A. Oh, Footnote 83 somewhere. Yeah, that's right. 13 In that particular document, I don't think it provides 14 enough information for me to understand the context of, 15 you know, how did he come to make that statement, and 16 exactly which system is he talking about, I don't think 17 we can know. 18 Q. And that's my only point, right, is that from 19 this one particular notation, you're not concluding 20 there was some enterprise-wide failure to implement the 21 principle of least privilege, you would just defer to 22 Mr. Quitugua's testimony. There was some particular 23 system or set of systems that was found not to be -- 24 A. Well, no. There were many other reasons why I 25 --</p> <p>202</p>	<p>1 sometimes it's to find things that are going well too. 2 Q. Sure. It's to make sure everything is going 3 well and if there's things that are not going well to 4 identify them from mitigation? 5 A. Sure. 6 Q. And like you said, it indicates in the right 7 that some of this remediation work was already completed 8 by the end of 2017? 9 A. Well, it says "Identify high-risk accounts" and 10 that's complete. It doesn't say that they remediated 11 anything having to do with the high-risk accounts, and 12 the stuff under it says: 13 "Track mediation not started, document 14 results and establish repeatable security 15 assessment, and methodology not started." 16 That's in that column. 17 Q. Correct. But these were -- obviously, the 18 intent here is to flag issues for eventual remediation? 19 A. Sure. 20 Q. And whatever specific issue this slide was 21 referring to, certainly the issue could have been 22 resolved by October 2018, which is the start of the 23 relevant period here? 24 A. I don't know. It would depend on the issue, 25 the system, how hard it was to fix it, all sorts of</p> <p>204</p>

Mark Graff
2/14/2025

<p>1 reasons.</p> <p>2 Q. But you don't know. You have no reason to</p> <p>3 believe it wasn't fixed by October 2018?</p> <p>4 A. Right, I agree with that.</p> <p>5 MR. TURNER: Okay. We've been going</p> <p>6 for a while. Do you guys want to break, you</p> <p>7 want to --</p> <p>8 MR. CARNEY: We'll leave it up to the</p> <p>9 witness.</p> <p>10 THE WITNESS: I could use a break, a</p> <p>11 short break.</p> <p>12 THE VIDEOGRAPHER: The time right now</p> <p>13 is 4:14 p.m., and we're off the record.</p> <p>14 (Whereupon, a short break was taken.)</p> <p>15 THE VIDEOGRAPHER: Stand by, please.</p> <p>16 The time right now is 4:28 p.m. We're back on</p> <p>17 the record.</p> <p>18 BY MR. TURNER:</p> <p>19 Q. Mr. Graff, let me show you another document you</p> <p>20 cite in your report.</p> <p>21 (Whereupon, SW-SEC00043620-630 was</p> <p>22 marked as Graff Exhibit 19, for identification,</p> <p>23 as of this date.)</p> <p>24 Q. I'm showing you a slide deck titled "User</p> <p>25 Access Management," bearing the date January 8, 2018,</p> <p>205</p>	<p>1 Q. Do you see how the slide deck is titled "Tool</p> <p>2 Evaluation and Recommendation"? That's part of the --</p> <p>3 if you turn to the first page.</p> <p>4 A. Yes, I see that.</p> <p>5 Q. And then the third page is a tool analysis?</p> <p>6 A. Yes.</p> <p>7 Q. And multiple witnesses testified in the case</p> <p>8 about how around this time -- around this time, the</p> <p>9 company was looking for a standardized tool it could use</p> <p>10 to automate the provisioning process.</p> <p>11 Do you remember that?</p> <p>12 MR. CARNEY: Objection. Foundation.</p> <p>13 A. Yes.</p> <p>14 Q. And the company moved to Azure AD or they</p> <p>15 started to move to Azure AD.</p> <p>16 Do you remember that testimony?</p> <p>17 A. I remember testimony about Azure AD and they</p> <p>18 were considering it and moving towards it, yes.</p> <p>19 Q. And you can see in page 5, there was a proposed</p> <p>20 recommendation about moving to Azure AD?</p> <p>21 A. I'm sorry, where are -- I'm looking at the</p> <p>22 page. Oh, there, it is, page 5.</p> <p>23 Q. Proposed recommendation?</p> <p>24 A. Yes, I see it.</p> <p>25 Q. And you see it talks about Azure AD there</p> <p>207</p>
<p>1 Bates stamp SW-SEC43620. The title is -- excuse me.</p> <p>2 Do you recognize this deck?</p> <p>3 A. It will just take me a moment to leaf through</p> <p>4 it.</p> <p>5 Q. Mm-hmm.</p> <p>6 A. It looks familiar. I don't remember precisely</p> <p>7 what's in it.</p> <p>8 Q. You cite the second page of this document where</p> <p>9 it says:</p> <p>10 "There is no organization-wide</p> <p>11 standardized approach to access management that</p> <p>12 includes provisioning, changing, and</p> <p>13 de-provisioning users' access to systems that</p> <p>14 contain personal information."</p> <p>15 I think that's down at the bottom of the slide.</p> <p>16 A. I see that quote. Could you help me by just</p> <p>17 make reference to my report?</p> <p>18 Q. Sure. It's in paragraph 78(a) of your report</p> <p>19 on page 39.</p> <p>20 A. I have it. Thank you.</p> <p>21 Q. Okay. Now, in terms of what exactly this slide</p> <p>22 deck concerned and what this language was intended to</p> <p>23 convey, do you remember the witness testimony about this</p> <p>24 slide deck?</p> <p>25 A. Not off the top of my head.</p> <p>206</p>	<p>1 having a single sign-on and being pre-integrated with</p> <p>2 custom and commercial applications?</p> <p>3 A. Yes, I see that.</p> <p>4 Q. And you're familiar with the concept of single</p> <p>5 sign-on, right?</p> <p>6 A. Yes.</p> <p>7 Q. So this means basically that, if you're</p> <p>8 provisioning a user with access, you don't have to</p> <p>9 provision -- you don't have to configure a number of</p> <p>10 different systems, you can just configure Azure AD and</p> <p>11 then it's integrated with all the other applications</p> <p>12 that they may need to use?</p> <p>13 A. Yeah, when it works like it supposed to, you</p> <p>14 don't need separate accounts in every system you are</p> <p>15 going to use. You can use one sign-on and be connected</p> <p>16 as you authenticate to the other systems.</p> <p>17 Q. Right. If that's what this slide deck was</p> <p>18 about, that there was a need for an organization-wide</p> <p>19 system like that to automate that provisioning process,</p> <p>20 again, that doesn't imply that there was any general</p> <p>21 failure to implement role-based access controls at the</p> <p>22 company?</p> <p>23 MR. CARNEY: Objection to form.</p> <p>24 A. I could imagine that customers would want to</p> <p>25 move to an integrated single sign-on system for many</p> <p>208</p>

Mark Graff
2/14/2025

<p>1 reasons, not necessarily because their role-based access 2 control has failed. 3 Q. Right. In fact, we talked about the SARFs 4 already, right? You could have like a manual process 5 where you get the SARF and then the IT people have to 6 provision the different systems separately. 7 You still have controls in place, they are just 8 more manual? 9 A. When it's done correctly, that can work; single 10 sign-on can simplify that. 11 Q. Okay. You also cite another document. 12 (Whereupon, SW-SEC00386134-143 was 13 marked as Graff Exhibit 20, for identification, 14 as of this date.) 15 Q. So I'm showing you what's been marked as Graff 16 Exhibit 20, and this is a slide deck titled "Information 17 Security Incident Review," bearing the date 18 September 2018 with a Bates stamp SW-SEC386134. 19 And in this deck you cite the last page of the 20 deck, and it says "Security program status." And then 21 specifically you cite the second to last bullet, 22 "Identity management role and privilege management," and 23 then it's in red, and I think you point to the text on 24 the other side of the slide, which indicates red means 25 limited or nonexistent?</p> <p>209</p>	<p>1 know that I have specific information on this particular 2 bullet. 3 Q. Well, you said the language is clear. But -- 4 first of all, let me just ask you, do you even know if 5 this was, you know, a draft or whether it was a final 6 version of this deck? 7 A. Offhand, I don't see any notation that it was a 8 draft. I see it was marked as confidential. 9 Q. Right. But you don't have, one way or another 10 of knowing whether this was even a final version or not? 11 A. Based on what I can see in front of me, it 12 looks like it was a presentation, but I don't know 13 without -- I'd have to double-check my notes in the 14 report on the providence of it to give me a chance to 15 evaluate the import of this and the weight to give to 16 it. 17 You said that was paragraph 71? 18 Q. Mm-hmm, 71(d) -- or excuse me -- 19 MR. CARNEY: 78, right? 20 A. 78 -- 21 Q. 78(d), excuse me. No. 78 -- 71(b) is what I 22 have. That doesn't make sense either. 23 A. I don't think -- is there a B in 71? 24 MR. CARNEY: 78(b). 25 THE WITNESS: 78(b), as in boy.</p> <p>211</p>
<p>1 A. Yes, I see it. 2 Q. All right. 3 A. And where was that referred to, by the way, in 4 my report, real briefly? 5 Q. 71, paragraph 71. 6 A. I'll look at that in a moment. Thank you. 7 Q. And you say: 8 "This is clearly inconsistent with the 9 assertion that role-based access controls are 10 implemented." 11 Now, again, as a -- this is a few words on the 12 slide deck, right? In order to understand what 13 specifically the issue was, you need to ask the person 14 who wrote the slide? 15 A. Well, I'm not sure I agree with that. I mean, 16 they're pointing out a problem on a status page, and I 17 have several examples of role and privilege management 18 problems. 19 Q. Okay. But in order to understand what was 20 signified by this particular bullet, how do you know? 21 A. Well, I don't know precisely what they meant by 22 this particular bullet. The language is clear, but as 23 to what particular incident among the ones that I knew 24 about that led to them putting that bullet together, I'd 25 have to look and see whether I can find it, but I don't</p> <p>210</p>	<p>1 MR. TURNER: I see. 2 MR. CARNEY: Yes, this is it. 3 Q. Okay. So now that you've looked at your notes, 4 you don't have any way of knowing whether this was a 5 draft that somebody prepared or whether this was a final 6 version? 7 A. Well, in the absence of a notation, I mean, 8 normally in my experience, if it's a draft, it'll say 9 "draft" on it, but it looks to be a finished 10 presentation. 11 Q. Okay. Now, again, just -- going back to the 12 meaning of this notation, all you have here is an 13 indication that red means "limited" or "nonexistent." 14 So, first of all, the meaning of this phrase 15 would depend on what "limited" means here, right? 16 A. Well, sure. The meaning of the phrase depends 17 on what the meanings of the words are. And if you take 18 that and compare that to what the security statement 19 says, as I have, they are discordant, right, they don't 20 agree. 21 Q. It depends on what's meant by "limited," sir. 22 What if "limited" means manual? 23 A. This says "limited" or "nonexistent." 24 Q. But it doesn't clarify in what respect it's 25 limited?</p> <p>212</p>

Mark Graff
2/14/2025

<p>1 A. I don't think it does.</p> <p>2 Q. And what if it's being highlighted in red</p> <p>3 because the IT folks wanted to highlight for management</p> <p>4 the need to make the transition to Azure AD?</p> <p>5 A. Yeah, I can't speculate under --</p> <p>6 Q. You don't know, right?</p> <p>7 A. I know what it says, and that's all I know for</p> <p>8 sure.</p> <p>9 Q. You know what it says, but you don't know</p> <p>10 exactly what it means or why it was put in there?</p> <p>11 A. Well, I know what it means to me.</p> <p>12 Q. You don't know exactly what this is referring</p> <p>13 to or exactly why the person who wrote it put it in this</p> <p>14 deck?</p> <p>15 A. Yeah, I think -- yeah, I agree with you. I</p> <p>16 think they were trying to say it was limited or</p> <p>17 nonexistent. As to exactly what's meant by that, they</p> <p>18 felt it was important enough to put it in the slide</p> <p>19 deck, but you're right, I don't know their motives for</p> <p>20 sure. They had the chance to say strong program or</p> <p>21 needs improvement. They didn't say that. They said</p> <p>22 "limited" or "nonexistent." If you think you just</p> <p>23 needed improvement, they might have put it in yellow.</p> <p>24 Q. And, sir, if it was limited in respect of being</p> <p>25 a manual process -- scratch that.</p> <p>213</p>	<p>1 A. Well, I can tell from other reports and other</p> <p>2 e-mails and other presentations some of the problems</p> <p>3 they might have been dealing with, but I don't know</p> <p>4 which specifically they had in mind when they wrote</p> <p>5 that.</p> <p>6 Q. And what other e-mails were you referring to?</p> <p>7 The ones we've looked through already?</p> <p>8 A. The role-based access control problems.</p> <p>9 Q. Uh-huh.</p> <p>10 A. Well, then I'd have to go back to the report</p> <p>11 and review the analysis of role-based access control.</p> <p>12 But I've already I think reported on some issue, as I</p> <p>13 opine, with role-based access controls. I don't know</p> <p>14 which one of those they might be specifically referring</p> <p>15 to in their presentation.</p> <p>16 (Whereupon, SW-SEC00001497-550 was</p> <p>17 marked as Graff Exhibit 21, for identification,</p> <p>18 as of this date.)</p> <p>19 THE WITNESS: And I did double-check</p> <p>20 what you said about role-based access control.</p> <p>21 It doesn't say anything about it being</p> <p>22 automated.</p> <p>23 MR. TURNER: Thank you.</p> <p>24 Q. Okay. I'm showing you another slide deck, this</p> <p>25 one titled "Security and Compliance Program Quarterly</p> <p>215</p>
<p>1 We talked earlier about the SARFs and there</p> <p>2 being many SARFs that you observed and the user access</p> <p>3 reviews and, et cetera. If someone concluded that that</p> <p>4 was -- strike that.</p> <p>5 The security statement did not make any</p> <p>6 representation as to whether SolarWinds' role-based</p> <p>7 access controls were automated or manual or not, right?</p> <p>8 A. I'd have to check, but I believe you're right.</p> <p>9 Why don't you go ahead on the presumption that that's</p> <p>10 correct.</p> <p>11 Q. Okay. So, again, if what this was highlighting</p> <p>12 was that the access controls were limited in that sense,</p> <p>13 there was no contradiction with what the security</p> <p>14 statement says?</p> <p>15 MR. CARNEY: Objection. Vague and</p> <p>16 foundation.</p> <p>17 A. Yeah, I think that would be very speculative on</p> <p>18 my part to agree with that. I mean, it seems to me that</p> <p>19 the clear reading is that there was a problem they were</p> <p>20 trying to point out.</p> <p>21 Q. But you don't know exactly what it was?</p> <p>22 A. Well, I can tell you --</p> <p>23 MR. CARNEY: Objection. Asked and</p> <p>24 answered.</p> <p>25 THE WITNESS: Thank you.</p> <p>214</p>	<p>1 Overview," bearing the date August 16, 2019, Bates stamp</p> <p>2 SW-SEC1497. And this is something you cite in paragraph</p> <p>3 78(c) of your report.</p> <p>4 A. Yes, I see it. Thank you.</p> <p>5 Q. Right. And you highlight that -- let me</p> <p>6 actually turn to the right page. It's page 11 of the</p> <p>7 document, but it's the one Bates stamped 1507.</p> <p>8 A. I have 1507 here.</p> <p>9 Q. Yeah, and in your report, you point to the fact</p> <p>10 that it's -- in the table at the bottom of the slide,</p> <p>11 for the category "Authentication authorization and</p> <p>12 identity management," the NIST maturity level is labeled</p> <p>13 a one, which corresponds to the key entry that says, "Ad</p> <p>14 hoc inconsistent or reactive approach."</p> <p>15 A. Yes, that's right.</p> <p>16 Q. Now, again, is it possible that what this was</p> <p>17 highlighting was the manual nature of the SARF process,</p> <p>18 and the company wanted to progress to a more automated</p> <p>19 system?</p> <p>20 MR. CARNEY: Objection. Foundation.</p> <p>21 Q. Let me ask it differently, Mr. Graff.</p> <p>22 Is one way a company can mature its controls is</p> <p>23 by making them more automated and more centralized?</p> <p>24 A. Yes, and I think the cybersecurity vendors</p> <p>25 would be happy if they did that, but, yes, that's often</p> <p>216</p>

<p>1 a very good way to do it.</p> <p>2 Q. So is it possible this is indicating a desire</p> <p>3 to mature in that way, from having a relatively manual</p> <p>4 system to a more automated system? And I'll refer you,</p> <p>5 Mr. Graff, to the second to last bullet at the top,</p> <p>6 which refers to, "Movement to make Azure AD</p> <p>7 authoritative source of identity, plan to enable</p> <p>8 Federation for all critical assets"? Is it possible</p> <p>9 that's what this is referring to?</p> <p>10 A. I don't think it's likely. Look at the top</p> <p>11 bullet. It says:</p> <p>12 "Access and privilege to critical</p> <p>13 systems and data is inappropriate. Need to</p> <p>14 improve internal processes and procedures."</p> <p>15 I don't read that as a reference to a need to</p> <p>16 automate it. It says that the access and privilege to</p> <p>17 critical system is inappropriate. There's other issues</p> <p>18 raised in that, too.</p> <p>19 Q. And, again, do you know what specific issues</p> <p>20 that bullet -- that top bullet is referring to?</p> <p>21 A. Well, I could give you a few examples of access</p> <p>22 and privilege to critical systems and data that's</p> <p>23 inappropriate.</p> <p>24 Q. Could it be that it was something like that,</p> <p>25 that several instances that occurred where access was</p> <p style="text-align: center;">217</p>	<p>1 what they intended to convey, to discredit that</p> <p>2 testimony?</p> <p>3 MR. CARNEY: Objection to form.</p> <p>4 A. Well, I've seen a lot of evidence that would</p> <p>5 justify a rating of 1. I don't think we'd go lower than</p> <p>6 1. You could go to a zero. I've seen a lot of evidence</p> <p>7 that would justify a rating of 1. As to whether or not</p> <p>8 they intended to make this a sales pitch for automation,</p> <p>9 that's just not what's in the report.</p> <p>10 Q. Mr. Graff, you keep saying you've seen a lot of</p> <p>11 evidence, a lot of evidence. Take through what we're</p> <p>12 talking about here. We've seen some Biz App developers</p> <p>13 temporarily get access to an internal billing system</p> <p>14 that they need to do their job. We've seen an effort to</p> <p>15 limit customer support access to customer systems, and</p> <p>16 then we've seen a bunch of documents where you say I'm</p> <p>17 not sure exactly what this is referring to, but you've</p> <p>18 said you're not assuming that it reflects any pervasive</p> <p>19 failure to implement role-based access controls.</p> <p>20 So what is this damning evidence that</p> <p>21 SolarWinds supposedly failed to implement role-based</p> <p>22 access control, if it that's even what you're claiming?</p> <p>23 MR. CARNEY: Objection. Argumentative</p> <p>24 and compound.</p> <p>25 A. Well, there's some examples you've asked me not</p> <p style="text-align: center;">219</p>
<p>1 inappropriate and that they're simply flagging a desire</p> <p>2 to improve the system?</p> <p>3 MR. CARNEY: Objection. Foundation.</p> <p>4 Q. To minimize error?</p> <p>5 A. I can interpret this and the words in front of</p> <p>6 me based on my experience. What they had in their minds</p> <p>7 when the wrote it, I can't speculate, but I can see that</p> <p>8 they are pointing out problems that need to be improved</p> <p>9 in access, privilege, critical systems and</p> <p>10 authentication and authorization and identity</p> <p>11 management.</p> <p>12 Q. And if the witnesses in this case who</p> <p>13 participated in putting this deck together testify that</p> <p>14 what was intended by this slide was that the company --</p> <p>15 there was a desire to automate access controls and</p> <p>16 centralize access controls to minimize error, would you</p> <p>17 have any reason to discredit that testimony?</p> <p>18 MR. CARNEY: Objection. Foundation.</p> <p>19 A. Well, that's not what they said in their</p> <p>20 presentation, but if you want to show me some testimony</p> <p>21 where they discuss it, I'll take a look.</p> <p>22 Q. I'll represent to you that there was testimony</p> <p>23 on this by Mr. Brown and Ms. Johnson. I'm asking you</p> <p>24 now to assume that's what the testimony was.</p> <p>25 Do you have any basis to contest that that was</p> <p style="text-align: center;">218</p>	<p>1 to get into, there's other areas of complication, but I</p> <p>2 can give you a couple of other examples that relate</p> <p>3 specifically to failures in role-based access control if</p> <p>4 you'd like.</p> <p>5 Q. What are they, please?</p> <p>6 A. Sure. Well the -- another failure of</p> <p>7 role-based access control, and this also pertains to</p> <p>8 practice of terminating employees -- Tim Brown has an</p> <p>9 e-mail -- I'd have to find it -- where he complains that</p> <p>10 a terminated employee, nevertheless, persists in having</p> <p>11 access to some Google Docs, and he complains in this</p> <p>12 e-mail, that says, you know, how could this happen --</p> <p>13 And I'm paraphrasing, that he still has access to these</p> <p>14 documents? And he also -- as my memory serves -- he</p> <p>15 also says that this is something that happens more</p> <p>16 frequently than he'd like. I'd have to find the exact</p> <p>17 quote.</p> <p>18 But that's an example of not only a termination</p> <p>19 problem but also role-based access control, since he</p> <p>20 shouldn't have access to the document based on his role</p> <p>21 as a former employee.</p> <p>22 Another example --</p> <p>23 Q. Can we stop there?</p> <p>24 A. Sure.</p> <p>25 Q. So SolarWinds had thousands of employees,</p> <p style="text-align: center;">220</p>

Mark Graff
2/14/2025

<p>1 sort of audit done relating to the concept of least 2 privilege? 3 A. It would seem to indicate that, yes. 4 Q. And in fact, in your own report, sir, you cite 5 that several other audits, for example, paragraph 120, 6 you cite an April 2018 e-mail circulating the results of 7 an internal audit relating to -- relating to privileges 8 for certain accounts? 9 A. I see paragraph 120, and I cite an internal 10 audit talking about shared SQL legacy login credentials. 11 Q. That should have to do with the principle of 12 least privilege? 13 A. Among other things. It has to do with SDL 14 also. 15 Q. And we've already talked about the user access 16 reviews that SolarWinds conducted? 17 A. It'd have to do about the shared access problem 18 too. 19 Yes, we have talked about user access reviews. 20 Q. Right. And that -- those user access reviews 21 were designed to check whether user access privileges 22 were properly set? 23 A. That would be the typical reason to do them. 24 And of course I don't know how exactly well they did 25 them, but that would be one of the reasons you do it,</p> <p>237</p>	<p>1 access? 2 MR. CARNEY: Objection to form. 3 A. Well, the sentence you read to me does indicate 4 that there was periodic audits of user contents related 5 to financial systems, I think the phrase was, which was 6 also the level of -- set of systems that referred to in 7 that password policy document Mr. Bliss gave me. 8 So it's significant financial systems, I think 9 was the quote? 10 Q. I think the more relevant words are including 11 active directory, which was the name identity store that 12 the company used to control its environment. Right? 13 A. Right. 14 Q. So is it possible, Mr. Graff, that Ms. Pierce 15 wasn't an expert, didn't have a good understanding of 16 the controls at issue, maybe it was just wrong that 17 there was no audit in place that had ever been performed 18 relating to the principle of least privilege? 19 A. She could have been misinformed and she 20 certainly could have made a mistake. I think there's a 21 lot of indication that there were issues either with 22 audits taking place or with the audits missing things. 23 But on the other hand, there were certainly some 24 periodic audits of some systems. 25 Q. Okay. So if she's wrong about this notation</p> <p>239</p>
<p>1 sure. 2 Q. And you actually cite to a -- the results of 3 one of those audits in paragraph 97 and note 180. 4 MR. CARNEY: The witness had asked for 5 a break a while ago. 6 THE WITNESS: If now would be a good 7 time. I could go for a few minutes longer, but 8 I certainly am looking forward to a break. 9 MR. TURNER: Okay. Just maybe three 10 more questions or so. 11 Q. We talked about the PwC audits that were done. 12 Do you remember those? 13 A. I remember you talking about them. I don't 14 remember reading the audit reports. 15 Q. And I can represent to you, sir, that one of 16 the controls PwC looked at, I'll just read it to you, 17 states: 18 "User access privileges are revalidated 19 on a quarterly basis to confirm that users 20 maintain appropriate access. These validation 21 procedures are performed for all financially 22 significant application systems including 23 active directory." 24 So would that also indicate that SolarWinds had 25 the practice of conducting audits related to user</p> <p>238</p>	<p>1 here, then you would withdraw your reliance on that 2 notation. Am I right to assume that? 3 A. If she was wrong about what? 4 Q. That an audit relating to the concept of least 5 privilege had never been performed? 6 A. Were we talking about -- 7 Q. Page 32. 8 A. Page 32. Let me just look at that again. 9 You've been moving me back and forth between several 10 documents. 11 Okay. So it says: An audit that this is in 12 place has never been performed. She's talking about 13 least privilege. 14 Q. So if she was wrong about that, you, of course, 15 would not rely on that notation for any conclusion of 16 yours? 17 A. Well, I'd be curious to know if it did happen, 18 you know, why she said it didn't, but -- but if there 19 was a quarterly review of least privilege from PwC, that 20 would be good. 21 MR. TURNER: Okay. We can take a 22 break. 23 THE VIDEOGRAPHER: The time right now 24 is 5:19 p.m. and we're off the record. 25 (Whereupon, a short break was taken.)</p> <p>240</p>

<p>1 THE VIDEOGRAPHER: Stand by, please. 2 The time right now is 5:34 p.m. and we're back 3 on the record. 4 BY MR. TURNER: 5 Q. Mr. Graff, before you mentioned that there were 6 a number of other access control categories in this Fed 7 Ramp assessment where Ms. Pierce indicated either there 8 was a program in place -- or excuse me, there may be a 9 program in place or that there wasn't a program in 10 place, to her knowledge. 11 Do you remember that? 12 A. Yes, I do. 13 Q. Now, a lot of these -- well -- strike that. 14 Are you -- do you have any familiarity with 15 Fed Ramp? 16 A. Some. 17 Q. Have you ever done any Fed Ramp certification? 18 MR. CARNEY: Objection. Vague. 19 Q. Have you done a Fed Ramp assessment, been able 20 to certify a company or a product as -- 21 A. I've never been certified. I've investigated 22 it some, but I've never been a certified Fed Ramp 23 participant. 24 Q. And you're aware Fed Ramp is a pretty demanding 25 standard for companies to meet?</p> <p style="text-align: center;">241</p>	<p>1 automatically --" and then it says: "Selection: 2 Removes, disables temporary and emergency accounts 3 after." And then it says: "Assignment, organization, 4 define time period for each type of account." 5 So this, again, is referring to some sort of 6 automation? 7 A. Yes. 8 Q. Which goes above and beyond what's in the 9 security statement, right? 10 A. The security statement talks about access 11 control and account management. It doesn't specifically 12 talk about automation. It talks about account 13 management. 14 Q. By the way, you see this term "information 15 system" that keeps popping up in the controls? 16 A. Yes. 17 Q. Do you know what that refers to? 18 A. Yes. 19 Q. What? 20 A. It's a term of art. It's defined in the NIST 21 documentation. And it can have two meanings: One is 22 this particular computer, and another is a set of 23 computers or even a network that perform a common 24 function. 25 Q. And do you know what it means in the context of</p> <p style="text-align: center;">243</p>
<p>1 A. Yes, I'd agree. 2 Q. And it's -- the certification is for particular 3 cloud products, right, that's what Fed Ramp is for? You 4 have to have that certification to sell a cloud product 5 to the federal government? 6 A. Yes, that's right. 7 Q. You mentioned those other categories, but a lot 8 of the other access control categories in this document 9 are about things that go above and beyond what's in the 10 security statement, right? 11 A. I'd have to review that quickly. 12 Q. Sure. Take a look at the, let's say, the third 13 page of the document where it says page 25 of 209. 14 A. I see it. 15 Q. Okay. So, for example, at the top, it says: 16 The organization employs automated mechanisms to support 17 the management of information system accounts. 18 You already mentioned earlier that the security 19 statement doesn't say anything about automation with 20 respect to rule-based access controls? 21 A. It doesn't specifically talk about automation 22 in the security statement, that's right. And that's not 23 the only way to do a good job on account management to 24 use automation. 25 Q. And then the next one: "The information system</p> <p style="text-align: center;">242</p>	<p>1 a Fed Ramp assessment? 2 A. It will depend a little bit on the context of 3 the particular Fed Ramp control they're talking about. 4 Q. Is it possible that the controls used the term 5 "information system" to refer to the cloud product being 6 evaluated? 7 MR. CARNEY: Objection. Vague. 8 A. Yeah, it would refer to the cloud product, but 9 it would also -- they're also very interested in -- Fed 10 Ramp in the systems on premises that interact with the 11 cloud. So it wouldn't be necessarily just the cloud 12 system. 13 Q. Take a look at page 38 of the document. 14 A. Yes, I see it. 15 Q. And it says: 16 "The information system: Displays to 17 users assignment organization define system use 18 notification message or banner before granting 19 access to the system that provides privacy and 20 security notices consistent with applicable 21 laws, executive orders and directives, 22 policies, regulations, standards and guidance, 23 and states that: One, users are accessing a 24 U.S. government information system." 25 I'll stop there.</p> <p style="text-align: center;">244</p>

Mark Graff
2/14/2025

<p>1 So in other words, this is saying this is some 2 control that requires the information to display a 3 banner to users that they're accessing a U.S. government 4 information system. Is that how you read it? 5 A. Let me just read the whole thing and I'll let 6 you know. 7 Q. Sure. 8 A. Yeah, that's not quite right. If I could take 9 a moment and just explain this notation, I think it 10 would be clear to everybody. 11 Q. The red notation? I'm talking about column F. 12 A. Yes, but I'm talking about the language in 13 letter A. This is -- in this document, I could explain 14 this in just 30 seconds, if I may. 15 Q. Go ahead. 16 A. In these NIST documents when they're talking 17 about control -- 18 Q. Why are we talking about NIST, by the way? 19 A. This is -- Fed Ramp is controlled by NIST. So 20 this is a federal document that comes under the aegis of 21 the National Institute of Standards and Technology, 22 which is responsible for setting standards for all 23 federal systems. 24 Q. Uh-huh. 25 A. So this is a convention used in these</p> <p>245</p>	<p>1 with your general characterization. 2 Q. So it's possible that when you have a number of 3 controls in here to talk about what the information 4 system has to do, it's not talking about SolarWinds 5 network or the organization as a whole, but whatever 6 cloud product is being evaluated for Fed Ramp purposes? 7 A. There's one of them that might well qualify 8 that way. 9 Q. Let's talk about passwords. 10 A. Okay. 11 Q. And in particular, the representation that 12 security statement stating: 13 "Our password best practices enforce 14 the use of complex passwords that include both 15 Alpha and numeric characters." 16 You would agree with that? 17 A. Yes. 18 Q. Now, you would agree that SolarWinds enforced 19 the use of complex passwords on active directory? 20 A. For most of their systems, they certainly could 21 have used active directory to do that. 22 Q. And in fact, you've reviewed evidence, haven't 23 you, that the company did do that in active directory, 24 that it set password complexity to be activated on 25 active directory?</p> <p>247</p>
<p>1 documents. And what they're trying to say is 2 assignment, and then it gives you this or that. The 3 person filling out the form is forced to assign a value, 4 either this or that. 5 And so what this is telling you is that if -- 6 in the case that it's a U.S. government system, they 7 need to supply that banner. But if the assignment is a 8 different kind of organization, you might need an 9 organization-specific banner. 10 Q. I don't think that's what it says, Mr. Graff. 11 The choice seems to be between a notification 12 message or a banner. 13 A. Yes. 14 Q. But the information system is required to 15 display to users that they're using an access -- that 16 users are accessing a U.S. government information 17 system. 18 A. In the case of a Fed Ramp system, yes, that 19 sounds right. 20 Q. Right. So the information system being 21 referred to here would be the cloud product that is 22 being sold, which needs to inform users of that product 23 that they're accessing a U.S. government system? 24 A. That's a -- that's a reasonable interpretation. 25 There are other systems that might apply to, but I agree</p> <p>246</p>	<p>1 A. I'm not recalling that on the top of my head, 2 but I think that's likely. 3 Q. Would it help to see the document? 4 A. It would help if we can do it quickly. I don't 5 want to hold things up. 6 Q. Okay. Well, you tell me, Mr. Graff, are -- 7 would you agree that SolarWinds enforced the complex -- 8 the password complexity setting on active directory? 9 A. I guess I'd like to see that. And it would be 10 -- only would be a point in time, anyway, of course, 11 but -- 12 (Whereupon, SW-SEC-SDNY_00055077 was 13 marked as Graff Exhibit 23, for identification, 14 as of this date.) 15 THE WITNESS: Thank you. I have this 16 document. 17 Q. Okay. So I'm showing you what's been marked as 18 Graff Exhibit 23. It's Bates stamped SW-SEC-SDNY_55077. 19 And it's a screenshot of the active directory settings 20 as of 11/6/2017. 21 Do you see that up top? 22 A. I see that. 23 Q. And then under -- on the row: "Password must 24 meet complexity requirements," the setting is enabled? 25 A. That's right.</p> <p>248</p>

<p>1 Q. So you would agree that as early as November 6, 2 2017, SolarWinds enforced password complexity in active 3 directory?</p> <p>4 A. Well, yeah, the screenshot clearly shows that, 5 at least as of that time, but I have no reason to 6 believe that they didn't use this setting in active 7 directory. Mind you, it only controls a certain subset 8 of their systems, but -- active directory. But yes, it 9 appears to be set that way.</p> <p>10 Q. It would control most of their systems, right, 11 that's how -- that was their primary identity store?</p> <p>12 MR. CARNEY: Objection. Vague.</p> <p>13 A. If you mean a numerical majority, I would think 14 so. You know, it's hard to know precisely what the 15 active directory domains -- that this is referred to. 16 Because they could have many domains. So it's the 17 default domain policy.</p> <p>18 But certainly, this is an indication that they 19 used complex passwords on a set of systems that were 20 controlled by active directory.</p> <p>21 Q. Which was their primary identity source?</p> <p>22 A. I think it was.</p> <p>23 Q. And are you aware that, again, PwC, audited 24 password complexity on financially significant systems 25 including active directory in their 2019 and 2020</p> <p style="text-align: center;">249</p>	<p>1 Q. It was on an FTP account on a third-party 2 server at Akamai, right?</p> <p>3 A. Right.</p> <p>4 Q. And you don't know, do you, whether it was 5 possible to automatically enforce password complexity on 6 that system?</p> <p>7 A. Well, when you say "enforce," do you mean 8 automatically enforce by software or do you mean 9 somebody actually taking control of the system and 10 ensuring that it was complex?</p> <p>11 Q. Well, I'm first talking about automatically 12 enforcing it.</p> <p>13 A. Yeah, I don't know for sure if you could 14 automatically enforce password complexity on an FTP 15 account.</p> <p>16 Q. So you'd have to rely on human compliance with 17 the password policy?</p> <p>18 A. Well, there are ways that you can automate the 19 checking of password complexity. So there's a 20 difference between regulating the setting of the 21 password like active directory does and being able to 22 check to see whether there is a complex password.</p> <p>23 And there are ways to do that that don't have 24 anything to do with active directory. You can run a 25 special software that checks that.</p> <p style="text-align: center;">251</p>
<p>1 audits?</p> <p>2 A. I don't recall that, but it wouldn't surprise 3 me.</p> <p>4 Q. Do you want to see that as well?</p> <p>5 A. If you tell me that that's what it says, I'm 6 okay with that factoid.</p> <p>7 Q. And they found no significant deficiencies with 8 respect to that control?</p> <p>9 MR. CARNEY: Objection. Form.</p> <p>10 Q. Do you agree with that?</p> <p>11 A. Yeah, I guess I'd have to see that if you want 12 me to agree to their finding. But the systems that are 13 under the control of active directory would tend to have 14 complex passwords enforced.</p> <p>15 Q. Okay. So you don't have any basis to contest 16 that password complexity was enforced on active 17 directory throughout the relevant period?</p> <p>18 A. For the systems under the control of active 19 directory, I think that's right.</p> <p>20 Q. Okay. And you've talked about the SolarWinds 21 123 password?</p> <p>22 A. Mm-hmm.</p> <p>23 Q. And that was not on an active directory 24 account, right?</p> <p>25 A. Correct.</p> <p style="text-align: center;">250</p>	<p>1 Q. Okay. Do you know whether there was some sort 2 of special way to automate the checking of it on this 3 FTP account on an Akamai server?</p> <p>4 A. It would be highly likely given the importance 5 of doing that and the professionalism of Akamai, which 6 I've used. I think there probably is a way of doing it 7 and automating it. I don't know if they did it.</p> <p>8 Q. What way would there be of automating checking 9 of the complexity of the password?</p> <p>10 A. Briefly, you can -- there's software available 11 everywhere that checks for password complexity, and you 12 can easily set up, I've done it many times, a script 13 that run periodically and can check the password 14 complexity of a given account.</p> <p>15 Q. Well, wouldn't you have to know what the 16 password is in order to check whether it's complex?</p> <p>17 A. No. Oddly enough you don't.</p> <p>18 Q. How would it know what password to check then?</p> <p>19 A. Yeah, it's a -- I'll just do it quickly.</p> <p>20 There's a system, a friend of my invented it, that -- 21 there's a system called password cracking. And the way 22 it works is that you do it -- you construct what might 23 be a simple password, and then you check to see whether 24 when you encrypt that password you get the same result 25 as what you find in the encrypted password file.</p> <p style="text-align: center;">252</p>

<p>1 And by doing that, you can do it hundreds of 2 thousands of times a second, it's possible to determine 3 whether or not it's a simple password or the complex 4 password. 5 Q. I think what you're referring to, Mr. Graff, is 6 where you have a hash in a password and you're trying to 7 see if it's a complex password or a simple password that 8 could be hacked? 9 A. That's one way to do it. 10 Q. But that's if you have a hashed password to 11 start with. 12 If you just have a system that has an account 13 on it and you have no indication of what the password 14 is, hash or not, there's nothing to check, right? 15 A. If you have control of the account, as the FTP 16 user would, it is possible to run software to determine 17 whether or not a password is easily guessed. 18 Q. Yeah, if you have control of the account, if 19 you have the person who has control of the password. 20 Again, that's a manual element that you'd need to have, 21 right? You'd need to have the person actually checking 22 the password. And that's -- that requires manual 23 compliance. 24 A. Well, I don't want to beat this to death. 25 There are, I think, ways to automate that check for</p> <p style="text-align: center;">253</p>	<p>1 matches that hash? 2 A. That's one of the main ways it works. 3 Q. Okay. Here we're not talking about having a 4 hash of a password, we're just talking about someone at 5 SolarWinds set this password on the account. 6 Is there any way that someone else at 7 SolarWinds at InfoSec would be able to automatically 8 check that password in some centralized fashion? 9 MR. CARNEY: Objection. Vague. 10 A. Well, when you say someone at SolarWinds, I'm 11 not quite sure who you're characterizing. If there's 12 somebody who has the password for the FTP account and 13 there's a system administrator whose job it is to check 14 that, I think there would be a way to check it. 15 Q. Okay. And whenever the password was created, 16 you don't know of any way to have automatically required 17 the password to be complex? 18 A. Yes, it -- I can imagine how it might happen, 19 but I certainly can't be sure that it would be 20 available. 21 Q. Okay. So for that part of the process, you'd 22 require the person who was creating the password to 23 manually make it complex; that's what you'd be depending 24 on? 25 A. In other words, if you want to enforce password</p> <p style="text-align: center;">255</p>
<p>1 password complexity on an FTP server. 2 Q. Well, sir, I'm not going to let it go. But so 3 far all you've described -- I'm well aware of password 4 cracking software. 5 The password cracking software is going to take 6 a hash password and to see if you can come up with a 7 plain text match that generates the hash, right? 8 MR. CARNEY: Are you talking about 9 Akamai having the password now? It's not 10 clear, your question. Objection, vague. 11 MR. TURNER: Mr. Graff has referred to 12 an automated way of checking passwords. 13 MR. CARNEY: And you've repeatedly said 14 you would have to have the password and it's 15 not clear who you're saying doesn't have the 16 password. 17 MR. TURNER: Thanks for the speaking 18 objection, but let me continue. 19 Q. You've talked about an automated way of 20 checking passwords, but what you've referred to is 21 password cracking software, right? 22 A. That's certainly one way to do it, yeah. 23 Q. And the way password cracking software works is 24 if you have a hash of a password, then the cracking 25 software determines if it can find the plain text that</p> <p style="text-align: center;">254</p>	<p>1 complexity, you're saying you'd have to have the person 2 that created the password follow that guideline? 3 Q. Right. 4 A. Yes, that sounds right. 5 Q. And human compliance is always subject to 6 error? 7 A. I agree with that. 8 Q. And this particular password, this would only 9 be one of many thousands of passwords that were used at 10 the company? 11 A. Well, there were certainly thousands of 12 passwords used at the company. There weren't thousands 13 of passwords being used for this FTP account. 14 Q. And we'll get to what the FTP account was used 15 for in a minute. 16 A. Okay. 17 Q. But this is only one noncomplex password that 18 you were able to find out of the thousands that would 19 have been used at the company? 20 A. Well, I wasn't looking for them. I was 21 reporting what others had detailed. And I do believe 22 there was another reference to the lack of password 23 complexity. If we look at my report, we can probably 24 find it. 25 But I believe there's another set of concerns</p> <p style="text-align: center;">256</p>

<p>1 about password complexity. I think maybe it was Eric 2 Quitugua that complained about it, but I'd have to 3 double check. But anyway, there's -- there will be an 4 annotation. It's a citation. 5 Q. Well, let's not leave that hanging, Mr. Graff. 6 A. Okay. 7 Q. Is there some other evidence of a noncomplex 8 password you want to point me to? 9 A. It seems to me there was a reference to that. 10 I could be mistaken, but I think in my main report I 11 believe I have a reference to password complexity 12 issues. Let's see. 13 So Section 62 begins the password section. It 14 seems to me there's a reference to a problem with 15 password complexity in one of the testimonies. I'll 16 have to look for it. Let's see. I'm around the 17 Footnote 214. Let's just see. It looks like we're 18 talking about unique account IDs. Let's see. 19 MR. CARNEY: You want to look at 20 paragraph 128? 21 THE WITNESS: I'm at 117. Let me see 22 128. 23 Yes, that's -- in 128 -- paragraph 128 24 does describe a problem with the login 25 credentials and plain text and so forth. But I</p> <p style="text-align: center;">257</p>	<p>1 that the password policy was followed 100 percent of the 2 time? 3 A. I agree, you're right. 4 Q. So you have no evidence that it was a frequent 5 occurrence at SolarWinds to use noncomplex passwords? 6 A. Frequent? I didn't really address frequency. 7 But -- see if I can agree with that. 8 I don't think I have evidence that shows it was 9 a frequent problem. 10 Q. And you've characterized this as a major 11 incident, right? 12 A. I don't remember if I used that word or not. 13 But it was certainly significant and a significant risk. 14 Q. All right. Well, let's talk about how major it 15 was. 16 A. Uh-huh. 17 Q. You raised the possibility that if an attacker 18 had discovered this password on GitHub, they could have 19 used the password to upload a malicious file to 20 SolarWinds' download's website? 21 A. Yes, that's my understanding of the issue that 22 Tim Brown raised in his e-mail. 23 Q. You say at paragraph 87: 24 "Anyone on the internet could upload 25 malicious software into this repository.</p> <p style="text-align: center;">259</p>
<p>1 was looking for a reference to password 2 complexity. It seems to me that there's 3 another reference to that. 4 MR. TURNER: Referring to Footnote 162 5 on page 50, Mr. Graff. 6 THE WITNESS: 162 -- 7 MR. TURNER: Footnote 162 at page 50. 8 THE WITNESS: Thank you. I'm getting 9 closer. Let's see. 10 Yes, this is the reference I had in 11 mind. Quitugua, who says -- and question, was: 12 "Are you aware of this SolarWinds 123 being 13 used," so forth. 14 And he said: "There may have been a 15 possibility that in the lab environment's 16 password, such as, you know, weak passwords 17 were in use." 18 Q. So he doesn't -- 19 A. And also Brown said: "I'm not saying that the 20 password policy was followed 100 percent of the time." 21 So those are the two quotes I was thinking of. 22 Q. Okay. Those aren't actual instances of 23 noncomplex passwords. That's Mr. Quitugua saying 24 possible that a weak password might be in the lab 25 environment and Mr. Brown saying that he wasn't saying</p> <p style="text-align: center;">258</p>	<p>1 SolarWinds customers would then download these 2 malicious files while thinking they were 3 downloading legitimate SolarWinds materials." 4 That's the theory? 5 A. That's my paraphrase of what Tim Brown -- the 6 worry that Tim Brown reported, and I'm sure we can find 7 his quotations to that sense. 8 Q. Okay. So the idea is that someone with this 9 password could upload a file -- a malicious file to the 10 SolarWinds website where files were available for 11 download, and then customers could mistakenly download 12 the files, thinking they were legitimate? 13 A. Yeah, that's the scenario Tim Brown was 14 pointing out, and I think that was a risk. 15 Q. And you say Mr. Brown was pointing it out. 16 You're citing the e-mail back and forth about this 17 issue, right? 18 A. Yes. 19 Q. You didn't cite any deposition testimony in the 20 case about it? 21 A. Well, not that I recall. I don't know that he 22 was asked about that in deposition. I don't remember. 23 Q. Yeah, none of the witnesses were ever asked 24 about this incident in depositions taken in this case. 25 Are you aware that?</p> <p style="text-align: center;">260</p>

<p>1 A. Well, I'm not aware of all the questions they 2 were asked, and I would not know offhand whether they 3 were asked about it or not.</p> <p>4 Q. Yeah. I can represent to you that no questions 5 were asked at depositions about the case -- in the case 6 about this incident. And, you know, the SEC made a big 7 deal about this incident in their complaint.</p> <p>8 Does it surprise you at all that they never 9 asked any questions about it at deposition?</p> <p>10 MR. CARNEY: Objection. Argumentative. 11 And he's got citations to investigative 12 testimony right there in his report.</p> <p>13 THE WITNESS: Right. Where is my 14 section that I talk about this, anybody?</p> <p>15 MR. CARNEY: You can look at paragraph 16 132.</p> <p>17 THE WITNESS: Yeah, I talk about this.</p> <p>18 A. And to respond to your question, I don't have 19 any control over the lawyers, and I'm not surprised when 20 they make a decision -- a legal decision of what to ask.</p> <p>21 Q. Okay. What if I had told you -- what if I tell 22 you now that if they had deposed someone who actually 23 knew about the facts of this matter, the testimony would 24 be that this account did not have the ability to upload 25 files to the SolarWinds website, in other words, to</p> <p style="text-align: center;">261</p>	<p>1 Q. Well, I can ask to you assume facts and then 2 ask you what your reaction is. That's all I'm asking 3 you to do here.</p> <p>4 A. Okay. It's hard to imagine that the 5 possibility of a file being overwritten can be ironclad. 6 There are many ways in which the permissions on a site 7 can be overridden.</p> <p>8 Q. I'm asking you to assume that this account did 9 not have the ability to overwrite files that had already 10 been uploaded. So given that, does that change your 11 view of the magnitude of the incident if you make that 12 assumption?</p> <p>13 MR. CARNEY: Objection. Foundation.</p> <p>14 A. You're asking me to make quite an assumption 15 because there are a great many security problems that 16 could make such a change possible. So you're asking me, 17 if I understand your question, to exclude all those 18 possibilities and accept the idea that the file 19 permissions would be effective in preventing that.</p> <p>20 Q. Correct. I'm asking you to assume facts and 21 then asking you if those facts are true, would it change 22 your view of the severity of the incident. So assume 23 that this account could not be used to overwrite some 24 SolarWinds file that was already available for download 25 to customers.</p> <p style="text-align: center;">263</p>
<p>1 downloads.SolarWinds.com?</p> <p>2 MR. CARNEY: Objection. Foundation.</p> <p>3 A. Yeah, that seems like -- I don't know, like a 4 double hypothetical. I don't know what they would have 5 testified.</p> <p>6 Q. Well, I'm going to ask you to assume that's 7 what the testimony would be. I'm going to ask you to 8 assume that this account could upload files to a staging 9 folder, an FTP folder, but the files would not be made 10 available on the download site as a result without 11 further action by SolarWinds personnel.</p> <p>12 So if you assume that fact, does that change 13 your view of the magnitude of this incident?</p> <p>14 A. If Mr. Brown's assessment was incorrect and the 15 facts are as you suggest, then, sure, it would change my 16 assessment of the impact of the event. It would still 17 be a serious problem.</p> <p>18 Q. And if I told you to assume that the account 19 did not have the ability to overwrite any files that 20 were already on the download site, so there was no way 21 of simply replacing files that were already there, 22 again, would that change your view of the magnitude of 23 the incident?</p> <p>24 MR. CARNEY: Objection. Foundation.</p> <p>25 A. Well, that's quite an assumption.</p> <p style="text-align: center;">262</p>	<p>1 Does that change your view of the severity of 2 the incident?</p> <p>3 MR. CARNEY: Objection. Foundation.</p> <p>4 A. It's really -- honestly, it's very difficult 5 for me to imagine a situation where that wouldn't be at 6 all possible. Now, let me say, in answer to your 7 question, if, in fact, it wasn't possible, and all of my 8 experience indicates it might well have been possible, 9 no matter what the file permissions were, if, in fact, 10 it wasn't possible to modify the file, yes, that would 11 definitely affect my interpretation.</p> <p>12 Q. And even assuming that an attacker could use 13 the account somehow to post a malicious file on the 14 downloads.com -- or downloads.SolarWinds.com site, would 15 you agree that SolarWinds software would never install 16 that software as an update because it wouldn't be 17 digitally signed with SolarWinds' private key?</p> <p>18 MR. CARNEY: Objection. Form.</p> <p>19 A. Would you please say that again? Because I 20 want to make absolutely sure I know what you're asking.</p> <p>21 Q. Sure. Well, let me ask you this: Are familiar 22 with the role of digital signatures and validating 23 software updates?</p> <p>24 A. Yes, I am.</p> <p>25 Q. You want to explain what the digital signature</p> <p style="text-align: center;">264</p>

1 process does and how it works?

2 **A.** Sure. One way to validate software that is in
3 a repository or a software that has been patched and so
4 forth, is to compare what's called "a mathematical check
5 sum." So the technique is, you take a file that's known
6 good, we run a mathematical algorithm over it that --
7 and there are many, many different types -- and that
8 produces a number, a special number, a very -- it's a
9 big number. It's a hexadecimal number. Very large.

10 And then what we do to check and see whether
11 the vendor will release that check sum and say this is
12 the number you ought to get when you run this check, and
13 then the customer, if they want to, can use the same
14 software and get a check sum, and then compare it to
15 what the vendor said the check sum should be.

16 **Q.** And the algorithm that runs that calculation,
17 right, it draws on the vendor's public key in order to
18 make sure that the software was --

19 **A.** Yes, quite often it does.

20 **Q.** -- was digitally signed?

21 **A.** So the vendor will sign it with their digital
22 key, and then we can check the digital signature using
23 software we have.

24 **Q.** Okay. And often vendors, if they have some
25 sort of automatic software update as part of their

265

1 software, that software is not going to install an
2 update unless the update mechanism confirms that the
3 software was digitally signed?

4 **A.** There's -- it's often the case that vendors and
5 customers will use software to check the digital check
6 sum and compare it as a guard against tampering.

7 **Q.** Right. So in this case, if you have a
8 malicious file posted on the SolarWinds website, a
9 customer could manually check it to make sure it was
10 digitally signed, or a SolarWinds installer, whatever
11 software their customer is running, would check the
12 program to see whether it was digitally signed before it
13 ever gets installed on the customer's system?

14 **A.** I saw in Mr. Brown's discussion of this where
15 he alluded to that possibility and whether or not -- and
16 perhaps the idea that it would protect their customers
17 because they could use check sums, and also he referred
18 to a fellow in the company that was running check sums
19 and trying to validate whether or not those files had
20 been tampered with.

21 Now, let me say it as clearly as I can: Those
22 methods, in my personal knowledge, are not full proof.

23 **Q.** Right so --

24 **A.** And it's possible to tamper with files and
25 still elude this method of detection.

266

1 **Q.** Right. They're not full proof, but it is a
2 form of compensated control that would help to minimize
3 the risk of the scenario you were alluding to before,
4 where you'd have lots of customers downloading malicious
5 software on their systems.

6 **A.** It's a good step to take. It's not full proof.
7 There are attackers who can defeat this method.

8 **Q.** Okay. So that also is a factor in assessing
9 the likelihood of this risk ever arising, is the
10 existence of compensating controls?

11 **A.** Yes. And one would also have to consider the
12 likelihood that a highly experienced attacker would
13 focus on this particular repository as a means of
14 delivering a tampered software.

15 **Q.** And there's no evidence that any bad actor ever
16 did obtain or use this password in any way, let alone
17 for successfully distributing malware, is there?

18 **A.** No, I don't believe there is any evidence that
19 it was done successfully, although as I say, it could
20 well have been done in a way that couldn't be detected.

21 **Q.** You don't have any evidence that that occurred,
22 though?

23 **A.** No, I don't.

24 **Q.** Mr. Graff, let's talk about the software
25 development lifecycle section of the security statement.

267

1 **A.** Sure.

2 **Q.** And this may not take very long. But I just
3 want to get clear on what you're contesting about that
4 section of the security statement, and specifically, I'd
5 like to follow on -- excuse me -- focus on the sentence
6 in the security statement that says:

7 "Our security development lifecycle
8 follows standard security practices including
9 vulnerability testing, regression testing,
10 penetration testing and product security
11 assessments."

12 Do you remember that sentence? It looks like
13 you're looking it up.

14 **A.** I am looking it up just to verify the wording,
15 but just give me a moment.

16 I have the paragraph. Could I hear that again,
17 please?

18 **Q.** Sure. It's the sentence that reads:

19 "Our secure development life cycle
20 follows standard security practices including
21 vulnerability testing, regression testing,
22 penetration testing, and product security
23 assessments."

24 Do you see that sentence?

25 **A.** Yes.

268

<p>1 Q. I know you've talked a lot about the OIP issue 2 in your report. We can get to that in a minute, but I'd 3 like to put it aside for now. Okay? I just want to 4 talk about the software development life cycle that the 5 company applied to its customer-facing products, okay? 6 Am I right that you're not contesting that 7 SolarWinds carried out vulnerability testing as part of 8 its software development lifecycle? 9 A. Yes, I think they do vulnerability testing in 10 many cases, probably most cases, in terms of product 11 development. 12 Q. And you're not contesting that SolarWinds 13 carried out penetration testing as part of its software 14 development lifecycle? 15 A. They carried out penetration testing. I have 16 comments about the way they did it and whether or not it 17 matched what they said they were doing, but yes, I think 18 they were doing penetration testing in most cases when 19 they developed software for production. 20 Q. The only thing I see in your report about 21 penetration testing is toward the very end of your 22 report, paragraph 188. 23 A. I see it. 24 Q. And you say: 25 "Mr. Brown testified that penetration</p> <p style="text-align: center;">269</p>	<p>1 because Mr. Brown testified that it may not have been 2 done 100 percent of the time? 3 A. Well, you connected those two things. They did 4 penetration testing I think most of the time. There 5 were issues with the penetration testing, as I point out 6 in the report, but they did it most of the time, I 7 think. 8 It's a little hard to tell because if you look 9 at the final security reviews, they are very 10 inconsistent when they talk about penetration testing 11 and whether it was, in fact, done. 12 Q. Okay. But you're not -- you're not asserting 13 that there was any pervasive failure to do penetration 14 testing as part of the secured development lifecycle? 15 A. I think they did penetration testing on 16 products quite often. There were, as I said, issues 17 with the way they did it and the effectiveness of it, 18 but yes, I think they did do penetration testing. It's 19 hard to tell precisely because of the way they reported 20 the tests that they did. 21 Q. So let me ask you about -- you said you have 22 some concerns about the way they did it. And, again, 23 the only thing you say about that in your report is that 24 customers found vulnerabilities through pen testing of 25 their own that SolarWinds didn't find in its pen</p> <p style="text-align: center;">271</p>
<p>1 testing may not have been done '100 percent of 2 the time.'" 3 So in other words, it wasn't perfect? 4 A. Well, you're paraphrasing. I mean, he said it 5 wasn't done a hundred percent of the time, and so 6 perfection would have required a hundred percent of the 7 time, so it wasn't, in that sense, perfect. Absolutely 8 true. 9 Q. But you're not suggesting that that makes the 10 security statement representation about pen testing 11 untrue? 12 MR. CARNEY: Objection. I'm just going 13 to note it's an entire paragraph. You read one 14 sentence. 15 MR. TURNER: I don't need the speaking 16 objection. I'm asking about penetration 17 testing. 18 MR. CARNEY: Right, which is what the 19 whole paragraph is about. 20 Q. Mr. Graff -- 21 A. What's your question, please? 22 Q. You're contention -- excuse me. 23 You're not suggesting that SolarWinds' 24 representation that it did penetration testing as part 25 of its software development lifecycle is untrue simply</p> <p style="text-align: center;">270</p>	<p>1 testing. 2 And so you're basically asserting that this 3 means that SolarWinds could have done pen testing 4 better? 5 A. Well, should I talk about my evaluation? 6 Should I talk about the pen testing a little bit? 7 Because you didn't ask a question. I'm sorry. 8 Q. No. I'm trying to understand what the argument 9 is here. So basically, you're saying that customers 10 found vulnerabilities through their own pen testing that 11 SolarWinds didn't find in its pen testing. That's the 12 issue that you're pointing to in this paragraph, right? 13 A. That's one of the issues, sure, that's the main 14 issue. Harry Griffiths talks about this, and I quote 15 him extensively, in his deposition, and he talks about 16 the fact that the SolarWinds customers -- there were 17 instances where the customers uncovered vulnerabilities 18 that SolarWinds had missed. 19 Q. Right. That's the only issue that you referred 20 to in this paragraph besides the Mr. Brown remark, 21 right? 22 A. Well, yeah, I think best practices would mean 23 that the company would modify the way it did pen testing 24 in order to do a better job of catching the 25 vulnerabilities that their customers were catching.</p> <p style="text-align: center;">272</p>

<p>1 Q. So it might or might not? You don't know 2 without more detail?</p> <p>3 A. I can't evaluate the Facebook vulnerability 4 testing and penetration testing without more information 5 than you can give me.</p> <p>6 Q. And similarly, if SolarWinds' customers are 7 finding bugs that SolarWinds itself didn't find, could 8 mean lots of things. Could mean they were using a 9 different pen testing tool, or they were looking at it 10 in some way that SolarWinds missed, but it doesn't 11 necessarily mean that SolarWinds had a bad penetration 12 testing program?</p> <p>13 MR. CARNEY: Objection. Compound.</p> <p>14 A. What I say in the report, aside from the point 15 I do make about customers, it's not best practice if 16 your customers are finding bugs you missed. That may 17 happen every once in a while.</p> <p>18 My point in the report was that if that 19 happens, the company should modify their testing to 20 catch up with their customers, right? Figure out what 21 the customers are doing that they're not doing and 22 modify their program to do that.</p> <p>23 Q. The SolarWinds' customers who pen tested 24 SolarWinds' software were doing a due diligence how 25 secure the software was, right?</p> <p style="text-align: center;">277</p>	<p>1 industry, exactly what they were looking for, what 2 features they needed, how much money they had, what 3 their budgets were, what their costs were. I just can't 4 figure that out.</p> <p>5 Q. Okay. But you're not aware of any instance 6 where a SolarWinds' customer pen tested software and 7 found bugs and concluded:</p> <p>8 "Oh, we're not going to use your 9 software because the fact that we're finding 10 bugs that you didn't catch is just too much of 11 a red flag"?</p> <p>12 A. I do remember an e-mail but I don't know that 13 it made my report. But since you ask, I do remember 14 seeing an e-mail sent to Tim Brown from a CEO from one 15 of their customers who complained about the 16 vulnerabilities that he was seeing and did threaten to 17 stop using the software if they didn't do a better job 18 of finding vulnerabilities. That was somewhere in the 19 Tim Brown correspondence that I saw.</p> <p>20 Q. Nowhere cited in the report?</p> <p>21 A. I didn't cite it in the report. But since you 22 brought it up.</p> <p>23 MR. CARNEY: Objection. Vague as to 24 cited. He's got an appendix of materials 25 attached to the report.</p> <p style="text-align: center;">279</p>
<p>1 MR. CARNEY: Objection, foundation.</p> <p>2 A. You said they were doing due diligence to test?</p> <p>3 Q. They were doing it due diligence to test for 4 themselves how secure the software was, right?</p> <p>5 MR. CARNEY: Same objection.</p> <p>6 A. I'm not sure why they were doing it. You would 7 think they were doing it to be careful.</p> <p>8 Q. If they weren't satisfied, they could have 9 taken their business elsewhere?</p> <p>10 A. That's a business -- I don't know enough about 11 SolarWinds' customers and what parts of the product line 12 they use and what the competition is to answer that 13 question.</p> <p>14 Q. You're aware that SolarWinds served nearly all 15 Fortune 500 companies during the relevant period?</p> <p>16 A. That sounds right.</p> <p>17 Q. And continues to do so today?</p> <p>18 A. That, I don't know.</p> <p>19 Q. Do you think all those companies would be using 20 the software if they thought that SolarWinds' 21 development process was insecure?</p> <p>22 MR. CARNEY: Objection. Calls for 23 speculation.</p> <p>24 A. Yeah, that's -- I'm not a position to diagnose 25 the buying decisions of those companies in that</p> <p style="text-align: center;">278</p>	<p>1 THE WITNESS: Yeah, thank you.</p> <p>2 Q. All right. The bottom line, Mr. Graff, you're 3 not contesting that pen testing was done most of the 4 time. You're basically contending that you think they 5 could have done a better job qualitatively with it, 6 fair?</p> <p>7 A. I'm going to just double check, but I think 8 that's right.</p> <p>9 My argument is, what I say in the opinion, that 10 since -- if customers often found vulnerabilities that 11 SolarWinds had missed before releasing its products, 12 this should have alerted SolarWinds leadership that its 13 own penetration testing was not following security best 14 practices as asserted in the security statement.</p> <p>15 And then, as I say, they should have adjusted 16 their penetration testing.</p> <p>17 Q. Yeah. And can I just get a clear answer to my 18 question?</p> <p>19 Your assertion is not that they failed to do 20 penetration testing as a regular practice, you're just 21 criticizing the quality of the penetration testing that 22 was done?</p> <p>23 A. And most of the time I think they did do 24 penetration testing as it relates to products.</p> <p>25 Q. With respect to regression testing, you're not</p> <p style="text-align: center;">280</p>

Mark Graff
2/14/2025

<p>1 contesting that SolarWinds conducted regression testing 2 as part of its software development lifecycle? 3 A. It's hard to tell precisely from the final 4 security reviews that I looked at because they're not 5 very specific about that. I think it's probably the 6 case that they did do regression testing as part of 7 their ordinary production software development 8 lifecycle, but it's not clear to me how often they did 9 it, how well they did it. 10 Q. Mr. Rattray cited that 2,000 JIRA tickets 11 reflecting regression testing being conducted. 12 Did you look at those at all? 13 A. I did review a few. 14 Q. Would you consider that to be evidence that 15 regression testing was done as a regular practice as 16 part of the secure development lifecycle? 17 A. I think it's -- yes, I think that is evidence 18 that they conducted regression testing with some 19 regularity. 20 Q. And you're not contesting that SolarWinds 21 conducted product security assessments as part of its 22 software development lifecycle? You referred to the 23 final security reviews earlier. 24 MR. CARNEY: Objection to form. 25 A. Yeah, I found that the -- and I think I</p> <p>281</p>	<p>1 discuss that. It may have been more in the rebuttal 2 report than it was in the original report since I was 3 responding to Dr. Rattray's discussions of those. 4 MR. BRUCKMANN: That might be pages 38 5 and 39 of the rebuttal report, Mark. 6 THE WITNESS: Yeah, thank you. And do 7 I have the rebuttal report here? 8 MR. CARNEY: Exhibit 2. I can hand you 9 my copy. 10 THE WITNESS: I have two. What page? 11 Paragraph 38, did you say? 12 MR. CARNEY: Page 38, paragraph 67. 13 THE WITNESS: All right. Thank you. 14 Paragraph 67. 15 Okay, I've reviewed that. Thank you 16 for your patience. 17 Q. So your criticism is that the documentation of 18 the reviews is not sufficiently clear? 19 MR. CARNEY: Objection. 20 Mischaracterizes testimony. 21 A. That's one of my concerns. But I think, you 22 know, I -- I took a look at the FSRs, and there were a 23 couple of problems that I noticed right away. 24 The first thing is that I didn't see a simple 25 explanation of exactly what was supposed to be in the</p> <p>283</p>
<p>1 mentioned in either the original report or in my 2 rebuttal, I found the format of the FSRs and the way 3 they carried out that, the way they documented it, could 4 be problematical, and so I'm not sure I can agree with 5 that last assertion. 6 Q. You found the way that carried out -- the way 7 they documented it to be problematical? 8 A. Yeah. 9 Q. Now, you know that these final security reviews 10 were printed out in a way that doesn't include all the 11 links to JIRA tickets that were related to the FSRs 12 because of a database change issue. 13 Are you aware of that? 14 A. I noticed that the final security review 15 documents listed in some cases links to evidence that 16 would support their report of the review, but rarely 17 included substantive details about the review or its 18 results. 19 Q. But you are aware that those linked documents 20 were produced by SolarWinds? 21 A. Some of them were, for sure. 22 Q. Did you review those documents? 23 A. Many of them. 24 Let's, if we may, just review quickly what I 25 had to say about the FSRs, too. I know that I did</p> <p>282</p>	<p>1 FSRs. I didn't see a description. I don't remember 2 reading one, at least, of what that process was supposed 3 to contain. 4 But more than that, having reviewed some dozens 5 of these FSR documents, I think I used the word 6 hodgepodge in my rebuttal in that there were so many 7 different ways it was organized and so many different 8 things that were referred to in these final security 9 reviews. Sometimes they would talk about the 10 penetration testing, sometimes they would talk about 11 regression testing, but many times they didn't supply or 12 even refer to the results. 13 So it was almost every FSR was in a different 14 format, had different paragraphs, different contents. 15 It was very -- they were very -- well, in a way 16 disorganized. 17 Q. And does the security statement say anything 18 about the documentation that would be used for security 19 reviews being done in a uniformed fashion across teams? 20 A. It doesn't. But it does talk about software 21 development, and it does talk about -- I'll have to find 22 the precise reading, but it's a reference to the best 23 practices or industry best practices. I'd have to find 24 my exact reference. 25 But it doesn't talk about the FSRs, but it does</p> <p>284</p>

<p>1 talk about the reviews they did.</p> <p>2 Q. And again, Mr. Graff, I want to emphasize, the</p> <p>3 FSRs would link to JIRA tickets that are often not</p> <p>4 reflected in what were produced.</p> <p>5 So did you look at the JIRA tickets that were</p> <p>6 cross-referenced in the FSRs?</p> <p>7 A. I looked at several of them.</p> <p>8 Q. And did they reflect testing or analysis of</p> <p>9 code and assessments of risks?</p> <p>10 A. Yes, many of them did.</p> <p>11 Q. And would you consider that reviewing the</p> <p>12 security of a product as a matter of substance</p> <p>13 regardless of the form?</p> <p>14 A. Well, review -- yes, it's a form of review.</p> <p>15 The important thing about a final security review, as</p> <p>16 described in the SDL, I mean, is -- I mean, there's</p> <p>17 a -- a final security review is an element of a</p> <p>18 well-managed SDL.</p> <p>19 And there are a great many steps that should be</p> <p>20 carried out in that review. And so I didn't find in the</p> <p>21 evidence about these reviews they were conducting that</p> <p>22 they were doing it in an organized way and doing</p> <p>23 it -- yes, security best practices are a mandated aspect</p> <p>24 of all development activities, it says here.</p> <p>25 And also, it says that they follow standard</p> <p style="text-align: center;">285</p>	<p>1 You're not a lawyer, are you, Mr. Graff?</p> <p>2 A. No.</p> <p>3 Q. You're not a linguist, right?</p> <p>4 MR. CARNEY: Objection. Vague.</p> <p>5 A. No.</p> <p>6 Q. You haven't been engaged as a linguistics</p> <p>7 expert or a legal expert by the SEC?</p> <p>8 A. That's right.</p> <p>9 Q. So in terms of understanding whether "our</p> <p>10 products" modifies the rest of the paragraph or a</p> <p>11 sentence, you don't have any more expertise than I do on</p> <p>12 that issue?</p> <p>13 MR. CARNEY: Objection. Calls for</p> <p>14 speculation.</p> <p>15 A. My goal in reading this and reporting on it is</p> <p>16 to, as I say, compare it to best practices and also to</p> <p>17 deliver my understanding as a security expert of what</p> <p>18 these representations are.</p> <p>19 Q. And as a security expert, you have some sort of</p> <p>20 special knowledge that allows you to interpret whether</p> <p>21 "our products" in the first sentence was meant to apply</p> <p>22 to the rest of the paragraph versus just that sentence?</p> <p>23 A. My expertise and my experience are enough to</p> <p>24 tell me that when it says it's a mandate aspect of all</p> <p>25 development activities -- remember, I've managed</p> <p style="text-align: center;">287</p>
<p>1 security practices. Well, these reviews are part of</p> <p>2 standard security practices and part of best practices.</p> <p>3 Q. Let's talk about the OIP.</p> <p>4 A. The Orion Improvement Program.</p> <p>5 Q. Very good.</p> <p>6 A. Yeah.</p> <p>7 Q. The security statement says:</p> <p>8 "We followed a fine methodology for</p> <p>9 developing secure software that is designed to</p> <p>10 increase the resiliency and trustworthiness of</p> <p>11 our products."</p> <p>12 Would you agree the term "products" typically</p> <p>13 refers to the things that a company sells to its</p> <p>14 customers?</p> <p>15 A. Yes.</p> <p>16 Q. And would you agree that's what's being</p> <p>17 referred to here?</p> <p>18 A. In that sentence.</p> <p>19 And in the sentence a couple lines later, it</p> <p>20 says that these "security best practices are a mandated</p> <p>21 aspect of all development activities." And that's what</p> <p>22 I pointed out in my report.</p> <p>23 So that's not restricted-to products.</p> <p>24 Q. Would you agree that the OIP software app -- by</p> <p>25 the way, let me back up there.</p> <p style="text-align: center;">286</p>	<p>1 software development groups, so all development</p> <p>2 activities to me is pretty clear.</p> <p>3 Q. All development activities in the context of a</p> <p>4 paragraph that is about:</p> <p>5 "The methodology for developing secure</p> <p>6 software to increase the resiliency and</p> <p>7 trustworthiness of our products."</p> <p>8 What special expertise do you have that allows</p> <p>9 you to opine that the sentence you were looking at</p> <p>10 applies to something beyond "our products"?</p> <p>11 Have you ever conducted a -- any sort of survey of how</p> <p>12 people interpret security statements?</p> <p>13 A. No.</p> <p>14 Q. Is it possible that other people might</p> <p>15 reasonably construe this language differently than you</p> <p>16 do?</p> <p>17 A. Well, other people might construe it</p> <p>18 differently. I think I was pretty reasonable. I'm not</p> <p>19 sure if they disagreed with what would be reasonable.</p> <p>20 That's kind of speculative.</p> <p>21 Q. Right, I'm the most reasonable person I know.</p> <p>22 Now, would you agree that the OIP software</p> <p>23 application was not a product that SolarWinds sold to</p> <p>24 customers?</p> <p>25 A. Yes, that's my understanding.</p> <p style="text-align: center;">288</p>

<p>1 Q. It ran on a SolarWinds server?</p> <p>2 A. Yes.</p> <p>3 Q. It was not involved in running Orion or</p> <p>4 delivering services to the Orion customer?</p> <p>5 A. My understanding is it intended to collect</p> <p>6 information from Orion customers and therefore it was a</p> <p>7 kind of a service.</p> <p>8 Q. It was designed to collect analytics from</p> <p>9 SolarWinds customers?</p> <p>10 A. Mm-hmm.</p> <p>11 Q. But it wasn't used to actually deliver the</p> <p>12 services that Orion provides?</p> <p>13 MR. CARNEY: Objection to form.</p> <p>14 A. Yes, I think that's right. It was -- it wasn't</p> <p>15 designed to deliver the services that Orion provides,</p> <p>16 that's right. And I have a note -- I think in a</p> <p>17 footnote here I talk about exactly what kind of data</p> <p>18 moved back and forth.</p> <p>19 Q. And you could have -- you know, by analogy, you</p> <p>20 have a mobile app that uses Google Analytics to collect</p> <p>21 analytics data from the app, right? Are you familiar</p> <p>22 with --</p> <p>23 A. Yes, I've had a little familiarity with that.</p> <p>24 Q. And if a company says it pen tests its mobile</p> <p>25 app, that doesn't mean it's pen testing Google</p> <p style="text-align: center;">289</p>	<p>1 A. In many cases.</p> <p>2 Q. -- pen test Google Analytics potentially?</p> <p>3 A. Well, I'd have to look at the details. You</p> <p>4 could certainly test some of it.</p> <p>5 Q. And you are aware that SolarWinds has a number</p> <p>6 of other Biz Apps besides OIP?</p> <p>7 A. Yes.</p> <p>8 Q. Like billing applications or like Salesforce</p> <p>9 extensions to create customer e-mail lists?</p> <p>10 A. Okay, I agree with that.</p> <p>11 Q. And you're not claiming SolarWinds should have</p> <p>12 put those under its secure development lifecycle?</p> <p>13 A. Well, I'm not sure I'm making any claim at all.</p> <p>14 But what the SolarWinds employees who talked</p> <p>15 about this in the e-mails that I saw, and I believe it</p> <p>16 was at least Tim Brown, it may have been Chris Day, they</p> <p>17 talked about OIP and its role in collecting data.</p> <p>18 Tim Brown, as I recall, decided that OIP should</p> <p>19 be under the SDL. And I don't remember which employee</p> <p>20 actually suggested that; it was either Mr. Quitugua or</p> <p>21 Mr. Day. But there were concerns about the security</p> <p>22 risks associated with it, and they advocated -- I think</p> <p>23 Mr. Brown decided or at least asked, that OIP be brought</p> <p>24 under the SDL perhaps in response to some of the risks</p> <p>25 that were pointed out.</p> <p style="text-align: center;">291</p>
<p>1 Analytics?</p> <p>2 A. That's a little different case than the one</p> <p>3 we're talking about.</p> <p>4 Q. Google Analytics is collecting the analytics</p> <p>5 data, right?</p> <p>6 A. Mm-hmm.</p> <p>7 Q. Orion Improvement Program collects analytics</p> <p>8 data.</p> <p>9 The point is they're two separate things from</p> <p>10 the application itself?</p> <p>11 A. Well, the OIP application was not a product. I</p> <p>12 agree with that.</p> <p>13 Q. Would you agree that if a company says it pen</p> <p>14 tests its mobile app and it uses Google Analytics to</p> <p>15 test -- excuse me, to collect analytics from its mobile</p> <p>16 app, no one is going to assume that the company pen</p> <p>17 tests Google Analytics?</p> <p>18 A. Well, this hypothetical company, does it</p> <p>19 develop the Google Analytics software?</p> <p>20 Q. No.</p> <p>21 A. So it's the company -- I'm sorry. Please</p> <p>22 continue.</p> <p>23 Q. Can you pen test a vendor's product?</p> <p>24 A. Yes, you can.</p> <p>25 Q. So you could --</p> <p style="text-align: center;">290</p>	<p>1 Q. So Mr. Graff, it's getting late, and I want to</p> <p>2 get you out of here, so if you could just answer the</p> <p>3 question I ask rather than the question you might want</p> <p>4 me to ask.</p> <p>5 I'm asking you: Are you making any claim that</p> <p>6 SolarWinds should have put any other application, any</p> <p>7 other Biz App application besides OIP under its software</p> <p>8 development lifecycle?</p> <p>9 A. No.</p> <p>10 Q. Okay. So -- and again, you're not contesting</p> <p>11 that SolarWinds generally applied its SDL to</p> <p>12 customer-facing products?</p> <p>13 A. Well, I don't recall saying that, I'm afraid.</p> <p>14 They had an SDL, what they described as an SDL,</p> <p>15 and it had several parts. Some of that was, you know,</p> <p>16 the pen testing we talked about and the regression</p> <p>17 testing we talked about.</p> <p>18 There were other parts of it that I think</p> <p>19 weren't consistently applied, as I discuss in my report.</p> <p>20 Q. Again, I want to get you out of here soon.</p> <p>21 In terms of what was covered by the SDL, you've</p> <p>22 pointed to OIP, but you're not making any claim that</p> <p>23 customer-facing products were not covered under the SDL,</p> <p>24 were not -- the SDL was not applied to customer-facing</p> <p>25 products?</p> <p style="text-align: center;">292</p>

Mark Graff
2/14/2025

1 MR. CARNEY: Objection to form.
2 **A.** I'd have to check the -- I really would have to
3 check that report for that precise detail.
4 MR. TURNER: Okay. Let's take a
5 10-minute break.
6 THE WITNESS: Is it okay if I make that
7 check?
8 MR. TURNER: Sure.
9 THE VIDEOGRAPHER: The time right now
10 is 6:43 p.m. and we're off the record.
11 (Whereupon, a short break was taken.)
12 THE VIDEOGRAPHER: Stand by, please.
13 The time right now is 6:50 p.m. and we're back
14 on the record.
15 MR. TURNER: I have no further
16 questions. Thank you, Mr. Graff.
17 MR. CARNEY: All right. Thanks. And I
18 have no questions, but the witness will read
19 and sign. Thank you.
20 THE VIDEOGRAPHER: The time right now
21 is 6:51 and we are off the record.
22 (Time Noted: 6:51 p.m.)
23
24
25

293

1 CERTIFICATE OF WITNESS
2
3 I, MARK GRAFF, do hereby declare under
4 penalty of perjury that I have read the entire
5 foregoing transcript of my deposition testimony,
6 or the same has been read to me, and certify that
7 it is a true, correct and complete transcript of
8 my testimony given on February 14, 2025, save and
9 except for changes and/or corrections, if any, as
10 indicated by me on the attached Errata Sheet, with
11 the understanding that I offer these changes and/or
12 corrections as if still under oath.
13 _____ I have made corrections to my deposition.
14 _____ I have NOT made any changes to my deposition.
15
16 Signed: _____
17 MARK GRAFF
18
19 Dated this _____ day of _____ of 20____.
20
21
22
23
24
25

294

1 C E R T I F I C A T E
2 S T A T E O F N E W Y O R K)
3) s s . :
4 C O U N T Y O F Q U E E N S)
5
6 I, BROOKE E. PERRY, a Notary Public
7 within and for the State of New York, do hereby
8 certify:
9 That MARK GRAFF, the witness whose
10 deposition is hereinbefore set forth, was duly
11 sworn by me and that such deposition is a true
12 record of the testimony given by such witness.
13 I further certify that I am not related
14 to any of the parties to this action by blood
15 or marriage; and that I am in no way interested
16 in the outcome of this matter.
17 IN WITNESS WHEREOF, I have hereunto set
18 my hand this 14th day of February, 2025.
19
20
21 -----
22 BROOKE E. PERRY
23
24
25

295

1 ERRATA SHEET
2 Deposition of: MARK GRAFF
3 Date taken: FEBRUARY 14, 2025
4 Case: SEC v. SOLARWINDS CORP., et al.
5 PAGE LINE
6 _____ CHANGE: _____
7 REASON: _____
8 _____ CHANGE: _____
9 REASON: _____
10 _____ CHANGE: _____
11 REASON: _____
12 _____ CHANGE: _____
13 REASON: _____
14 _____ CHANGE: _____
15 REASON: _____
16 _____ CHANGE: _____
17 REASON: _____
18 _____ CHANGE: _____
19 REASON: _____
20 _____ CHANGE: _____
21 REASON: _____
22 _____ CHANGE: _____
23 REASON: _____
24 Signed _____
25 Dated _____

296

Errata Sheet

Matter: *SEC v. SolarWinds et al.*
Case No. 23-cv-9518-PAE

Deposition Date: February 14, 2025

Deponent: Mark Graff

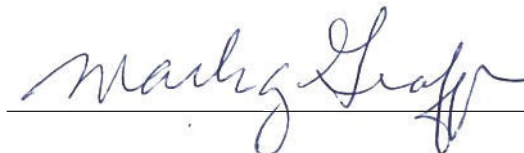
I have reviewed the transcript of my deposition taken in the above-referenced matter, which was supplied to counsel on March 3, 2025. I request that the following changes be entered upon the record for the reasons indicated. I authorize you to attach this Errata Sheet and the attached Acknowledgement of Deponent to the original transcript of my deposition.

<u>Page</u>	<u>Line No.</u>	<u>Now Reads</u>	<u>Should Read</u>	<u>Reason</u>
8	11	every eight years	over eight years	Typo
11	5	Did have people calling in	Did you have people calling in	Clarity
11	12-13	We talked a lot of about	We talked a lot about	Clarity
13	11	“system securities”	“System Security”	Typo
14	6	Well, any other other than the ones	Well, any other – other than the ones	Clarity
14	16	FCC	FTC	Typo
16	9	built	rebuilt	Typo
17	13	anything Sunburst or SolarWinds	anything about Sunburst or SolarWinds	Clarity
23	3	Use the SELC	Use of SDLC	Typo
28	1	is are	is: are	Clarity
28	23	issues raised	issues were raised	Clarity
32	8	as as many	are as many	Typo
33	5	depends on my	depends on that	Clarity
33	10	correctly or they weren’t consistent with passwords and	correctly, or they weren’t consistent with passwords, and	Clarity
35	13	“Is a	“A	Quote from exhibit
35	17-18	respect to these five areas.”	respect to” these five areas.	Quote from exhibit
36	11	that,	that	Quote from exhibit
40	9	I may have seen every file	I may not have seen every file	Typo
44	1	risk assessment	risk acceptance	Typo
44	9	risk assessment	risk acceptance	Typo
44	12	assessment	acceptance	Typo
51	19	SolarWinds’ employees reported to	SolarWinds employees and reported to	Clarity
52	25	account in	account on	Typo
57	10	there’s significant issues	there are significant issues	Typo

57	11	that identified by	that were identified by	Clarity
58	24-25	issue that is slipped	issues that slipped	Typo
60	14	I agree that.	I agree with that.	Typo
61	14	security	cybersecurity	Quote from exhibit
64	7	accessed information	access to information	Typo
64	25	access information systems	access to information systems	Typo
66	2	access controls are	access controls that are	Clarity
67	3	different	difference	Typo
68	6-7	they did that often, they did it correctly.	they did that—often, they did it correctly.	Typo
69	17	SolarWinds’ employees	SolarWinds employees	Typo
79	13	in taking	and take	Quote from exhibit
79	15	and	or	Quote from exhibit
79	16	business	businesses	Quote from exhibit
83	5	business continuity issues	business continuity systems	Typo
88	24	process	processes	Quote from exhibit
90	20	in the markets	of the markets	Quote from exhibit
92	9	and they will. If they’re	and if they’re	Clarity
98	22	incident.	incident?	Typo
101	15, 20	853	800-53	Typo
102	2	853	800-53	Typo
104	6	There’s a National Institute of Standards of	The National Institute of Standards and	Typo
109	9	800171	800-171	Typo
117	4	entering	Including	Clarity
118	14	securities	security	Typo
120	6	referring to a specific technical standards	referring to specific technical standards	Typo
133	9	through the monitor	for the word “monitor”	Clarity
138	25	assist	systems	Quote from exhibit
145	13	evidence to	evidence either to	Quote from exhibit
148	18	that	the	Typo
149	20	not my evidence	not my testimony	Clarity
149	23	my twin conclusions	my two conclusions	Typo
155	8	SOCs	SOX	Typo
156	10	bare	bear	Typo
163	4	backup for 365	Backup O365	Typo
163	6	Biz Apps would use access	BizApps would use to access	Typo
163	7	backup billing and for backup of 365	Backup billing and for Backup O365	Typo
167	11	backup	Backup	Typo
167	14	right permissions	write permissions	Typo
167	16	And then Benefits of Accepting This Risk	And then under “Benefits of Accepting This Risk”	Clarity
168	20-21	access certain	access to certain	Clarity
188	3	Ronnie	Rani	Typo

201	21	case.	case?	Quote from exhibit
201	23	identified that weren't, you	identified, they weren't – you	Quote from exhibit
203	20	accounts,	accounts,”	Typo
203	21	November 2017.”	November 2017.	Typo
204	13-15	“Track mediation not started, document results and establish repeatable security assessment, and methodology not started.”	“Track remediation” - “Not Started,” “Document results and establish repeatable security assessment and methodology” - “Not Started.”	Quote from exhibit
209	22	Identity management role and privilege	Identity Management – Role and Privilege	Quote from exhibit
211	14	providence	provenance	Typo
218	7	when the wrote	when they wrote	Typo
221	6	Ronnie	Rani	Typo
222	16	Ronnie	Rani	Typo
223	14, 17	SolarWinds 123	solarwinds123	Typo
223	22	Ronnie	Rani	Typo
224	4	Ronnie	Rani	Typo
224	8-9	SolarWinds 123	solarwinds123	Typo
233	21	omissions	missions	Typo
234	5	this is place	this is in place	Typo
235	11	this place has never been informed	whether this was in place has never been performed	Clarity and Typo
235	22	It as	It was	Typo
239	11	name	main	Typo
242	20	rule-based	role-based	Typo
247	19, 21, 23, 25	active directory	Active Directory	Typo
248	8, 19	active directory	Active Directory	Typo
249	3, 6-7, 8, 15, 20, 25	active directory	Active Directory	Typo
250	13, 16-17, 18-19, 23	active directory	Active Directory	Typo
250	20-21	SolarWinds 123	solarwinds123	Typo
251	21, 24	active directory	Active Directory	Typo
252	20	friend of my	friend of mine	Typo
254	6	a hash password	a hashed password	Typo
257	13	Section 62	page 62	Clarity
258	12	SolarWinds 123	solarwinds123	Quote from exhibit
258	15	environment's	environments	Quote from exhibit
263	5	possibility	impossibility	Typo
264	21	Are familiar	Are you familiar	Typo
266	22	full proof	foolproof	Typo
267	1, 6	full proof	foolproof	Typo
268	7	security	secure	Quote from exhibit
271	14	secured	secure	Typo

278	24	I'm not a position	I'm not in a position	Typo
286	8	a fine methodology	a defined methodology	Quote from exhibit
286	23	restricted-to	restricted to	Typo
287	24	mandate	mandated	Typo



Mark Graff

April 1, 2025

Date